

Astaro Security Gateway V6.3

WebAdmin

Benutzerhandbuch

Astaro Security Gateway V6.3

(Software Version 6.303)

Benutzerhandbuch

Release 3.03 – Datum: 13.09.2006

Amalienbadstraße 36/Bau 33a, 76227 Karlsruhe, Germany
http://www.astaro.com

Einschränkung der Gewährleistung

Für die Richtigkeit des Inhalts dieses Handbuchs wird keine Garantie übernommen. Hinweise auf Fehler und Verbesserungen nehmen wir gerne unter der E-Mail-Adresse documentation@astaro.com entgegen.

Inhalt **Seite**

1. Willkommen bei Astaro 10
2. Einführung in die Technologie 11
3. Installation 20
3.1. Systemvoraussetzungen 21
3.2. Installationsanleitung 25
3.2.1. Software installieren 25
3.2.2. Sicherheitssystem konfigurieren 30
4. WebAdmin-Werkzeuge 39
4.1. Info-Box 39
4.2. Das Verzeichnis 40
4.3. Menü 40
4.3.1. Die Statusampel 40
4.3.2. Das Auswahlfeld 41
4.3.3. Die Auswahltabelle 42
4.3.4. Das Drop-down-Menü 43
4.3.5. Das Hierarchiefeld 43
4.4. Online-Hilfe 45
4.5. Refresh 45
5. System benutzen & beobachten 46
5.1. Grundeinstellungen (System) 48
5.1.1. Settings 48
5.1.2. Licensing 56
5.1.3. Up2Date Service 60
5.1.4. Backup 69
5.1.5. Anti-Virus (AV) Engines 77
5.1.6. SNMP 79
5.1.7. Remote Syslog Server 81

Inhalt Seite
5.1.8. User Authentication 83
5.1.8.1. Local Users 85
5.1.8.2. Novell eDirectory 86
5.1.8.3. RADIUS.. 91
5.1.8.4. SAM – NT/2000/XP 96
5.1.8.5. Active Directory/NT Domain Membership............ 98
5.1.8.6. LDAP Server.. 102
5.1.9. WebAdmin Settings 116
5.1.10. WebAdmin Site Certificate 119
5.1.11. High Availability 122
5.1.12. Certifications 129
5.1.13. Shut down/Restart 132
5.2. Netzwerke und Dienste (Definitions)................. 134
5.2.1. Networks 134
5.2.2. Services 141
5.2.3. Users 146
5.2.4. Time Events 150
5.3. Netzwerkeinstellungen (Network)..................... 152
5.3.1. Hostname/DynDNS... 152
5.3.2. Interfaces 154
5.3.2.1. Standard Ethernet Interface 159
5.3.2.2. Additional Address on Ethernet Interface 166
5.3.2.3. Virtual LAN 168
5.3.2.4. PPPoE-DSL-Verbindung 174
5.3.2.5. PPTPoE/PPPoA-DSL-Verbindung 179
5.3.2.6. PPP over Serial Modem Line 185
5.3.3. Bridging 191
5.3.4. Routing 194

Inhalt Seite

5.3.5. NAT / Masquerading 198
5.3.5.1. NAT 198
5.3.5.2. Masquerading 202
5.3.5.3. Load Balancing 204
5.3.6. DHCP Service 206
5.3.7. PPTP VPN Access 212
5.3.8. Accounting 220
5.3.9. Ping Check 221
5.4. Intrusion Protection 223
5.4.1. Settings 223
5.4.2. Rules 226
5.4.3. Portscan Detection 230
5.4.4. DoS / Flood Protection 234
5.4.5. Advanced 241
5.5. Paketfilter (Packet Filter) 243
5.5.1. Rules 243
5.5.2. ICMP 256
5.5.3. Advanced 260
5.6. Application Gateways (Proxies) 268
5.6.1. HTTP 269
5.6.1.1. Content Filter (Surf Protection) 279
5.6.2. SMTP 304
5.6.2.1. Content Filter 315
5.6.2.2. Spam Protection 320
5.6.3. POP3 330
5.6.3.1. Content Filter 332
5.6.4. DNS 336
5.6.5. Generic 338
5.6.6. SIP 340
5.6.7. SOCKS 344

Inhalt Seite
5.6.8. Ident 346
5.6.9. Proxy Content Manager 347
5.7. Virtual Private Networks (IPSec VPN) 355
5.7.1. Connections 365
5.7.2. Policies 374
5.7.3. Local Keys 379
5.7.4. Remote Keys 382
5.7.5. L2TP over IPSec 386
5.7.6. CA Management 389
5.7.7. Advanced 394
5.8. System Management (Reporting) 398
5.8.1. Administration 398
5.8.2. Virus Statistics 399
5.8.3. Hardware 400
5.8.4. Network 401
5.8.5. Packet Filter 401
5.8.6. Content Filter 402
5.8.7. PPTP / IPSec VPN 402
5.8.8. Intrusion Protection 402
5.8.9. DNS 402
5.8.10. SIP 403
5.8.11. HTTP Proxy Usage 403
5.8.12. Executive Report 404
5.8.13. Accounting 405
5.8.14. Advanced 407
5.9. Remote Management (Remote Management) 410
5.9.1. Astaro Command Center (ACC) 410
5.9.2. Astaro Report Manager (ARM) 411

Inhalt | Seite

5.10. Local Logs (Log Files) 417
5.10.1. Settings 417
5.10.2. Local Log File Query 421
5.10.3. Browse 422
5.10.3.1. Log-Files 426
5.10.3.2. Notification Codes 431
5.10.3.3. HTTP Proxy Meldungen 462
5.11. Online Help / User Manual 465
5.11.1. Search 465
5.11.2. Glossary 465
5.11.3. User Manual 466
5.12. Firewall verlassen (Exit) 466
Glossar 467
Index 475
Notizen 484

1. Willkommen bei Astaro

Wir begrüßen Sie herzlich als neuen Kunden unseres Internet-Sicherheitssystems **Astaro Security Gateway V6**.

Dieses Handbuch führt Sie schrittweise durch die Installation des Internet-Sicherheitssystems, erklärt Ihnen ausführlich die Bedienung des Internet-Sicherheitssystems durch das web-basierte Konfigurationstool WebAdmin™ und unterstützt Sie bei der Dokumentation Ihrer Konfiguration.

Die aktuelle Version dieses Benutzerhandbuchs, können Sie von der **Astaro Knowledgebase** unter folgender Internetadresse herunterladen:

http://www.astaro.com/kb

Die Benutzerhandbücher und die Zusatzdokumentation (*Guides*) zur **Astaro Security Gateway** Software finden Sie über die Navigation auf der linken Seite im Unterverzeichnis **Astaro Manuals and Guides**.

Um Sie über aktuelle Informationen und Neuerungen auf dem Laufenden zu halten, beinhaltet dieses Handbuch auch Verweise auf Internetadressen von Astaro sowie weiteren Anbietern. Diese Internetadressen können sich allerdings auch ändern, bzw. im Falle der Fremdanbieter auch ganz entfallen.

Sollten Sie Fragen haben oder Fehler im Handbuch entdecken, zögern Sie bitte nicht und kontaktieren uns unter folgender E-Mail-Adresse:

documentation@astaro.com

Wenden Sie sich für weitere Informationen an unser User-Forum unter der Internetadresse ...

http://www.astaro.org

... oder greifen auf die Astaro Support Angebote zurück.

2. Einführung in die Technologie

Bevor auf die Funktionsweise und Handhabung des Internet-Sicherheitssystems **Astaro Security Gateway** eingegangen wird, möchten wir Ihnen einen Einblick geben warum ein derartiges System zum Schutz des Netzwerks erforderlich ist und welche Probleme und Gefahren ohne ein entsprechendes Sicherheitssystem bestehen.

Netzwerke

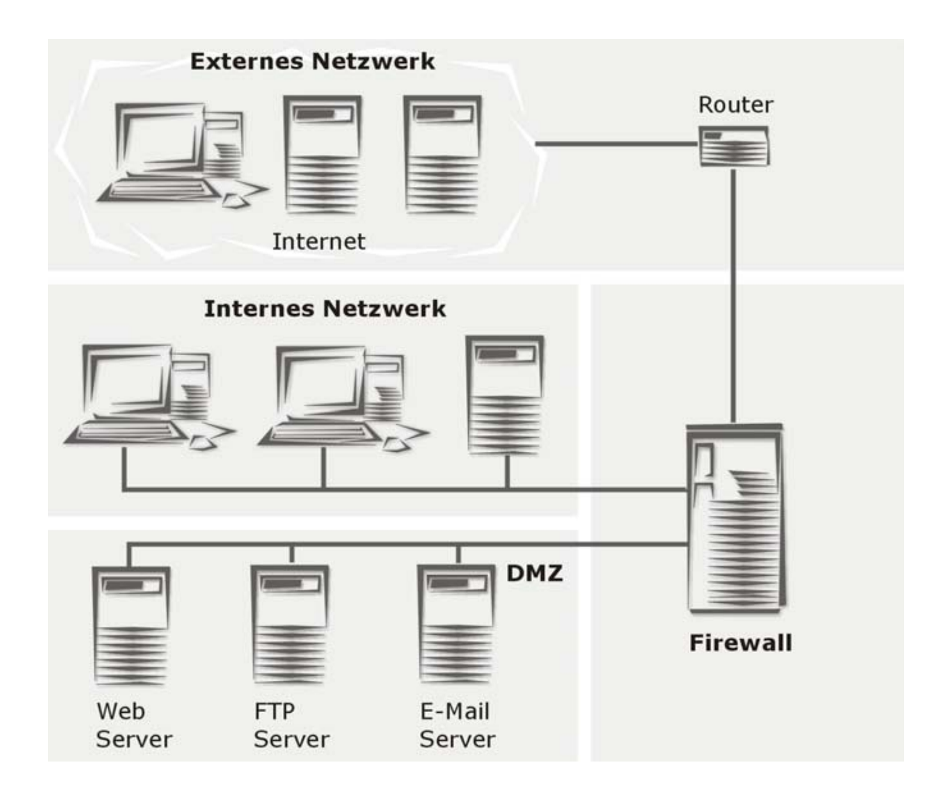
Das Internet ist heute als Schlüsseltechnologie für Kommunikation, Informationsbeschaffung, als Speichermedium für Wissens- und Erfahrungswerte sowie als Marktplatz für Informationsdienste etabliert. Seit seinen Anfängen haben sich seine Ausmaße vervielfacht und von 1995 bis 2003 war das zahlenmäßige Wachstum allein der .de-Domains nahezu exponential.

Die Endsysteme im weltumspannenden Netzwerk kommunizieren über das **Internet Protocol (IP)** und verschiedene andere Protokolle, die darauf aufsetzen z. B. TCP, UDP, ICMP. Basis einer solchen Kommunikation sind die IP-Adressen mit der Fähigkeit, alle erreichbaren Einheiten im Netzwerk eindeutig zu identifizieren.

Das Internet selbst existiert als Zusammenschluss verschiedenartiger Netzwerke, die sich sowohl durch die verwendeten Protokolle als auch durch die Ausbreitung unterscheiden. An Knotenpunkten, die zwei oder mehrere Netzwerke miteinander verbinden, entstehen eine Vielzahl von Aufgaben, die von Routern, Bridges oder Gateways übernommen werden. Ein spezieller Fall eines solchen Knotenpunktes ist die Firewall. Hier treffen in aller Regel drei Typen von Netzwerken aufeinander:

- Externes Netzwerk/Wide Area Network (WAN)
- Internes Netzwerk/Local Area Network (LAN)
- De-Militarized Zone (DMZ)

Eine Beispiel-Konfiguration sehen Sie auf der nächsten Seite.



Die Firewall

Ein Modul dieses Internet-Sicherheitssystems ist die Firewall. Die charakteristischen Aufgaben einer Firewall als Schnittstelle zwischen WAN, LAN und DMZ sind:

- Schutz vor unbefugten Zugriffen
- Zugangskontrolle (wer darf wie und worauf zugreifen)
- Beweissicherheit gewährleisten
- Protokollauswertung durchführen
- Alarmierung bei sicherheitsrelevanten Ereignissen
- Verbergen der internen Netzstruktur
- Entkopplung von Servern und Clients durch Proxies

- Vertraulichkeit/Abhörsicherheit von Daten gewährleisten

Es existieren nun mehrere generische Netzwerkeinrichtungen, die unter dem Überbegriff **Firewall** zusammengefasst, diese Aufgaben übernehmen. Im Folgenden soll kurz auf einige Formen und ihre Ableger eingegangen werden:

Netzwerkschicht-Firewalls: Paketfilter (Packet Filter)

Wie der Name schon sagt, werden hier IP-Pakete (bestehend aus Adressinformation, einigen Flags und den Nutzdaten) gefiltert. Mit einer solchen Firewall können Sie, basierend auf verschiedenen Variablen, Zugang gewähren oder ablehnen. Diese Variablen sind u. a.:

- die Ursprungsadresse
- die Zieladresse
- das Protokoll (z. B. TCP, UDP, ICMP)
- die Port-Nummer

Dieser Ansatz bietet große Vorteile: Seine Geschwindigkeit bei der Bearbeitung der Pakete und er ist betriebssystem- und applikationsneutral.

In der fortgeschrittenen und komplexeren Entwicklungsform umfasst der Leistungsumfang von Paketfiltern die Interpretation der Pakete auf höherer Kommunikationsebene. In diesem Fall werden Pakete auch auf Transportebene (TCP/UDP) interpretiert und Statusinformationen für jede aktuelle Verbindung werden bewertet und festgehalten. Dieses Vorgehen wird als **Stateful Inspection** bezeichnet.

Der Paketfilter merkt sich den Zustand jeder einzelnen Verbindung und lässt nur Pakete passieren, die dem aktuellen Verbindungszustand entsprechen. Besonders interessant ist diese Tatsache für Verbindungsaufbauten vom geschützten in das ungeschützte Netzwerk:

Baut ein System im geschützten Netzwerk eine Verbindung auf, so lässt der **Stateful Inspection Packet Filter** z. B. Antwortpakete des

externen Hosts in das geschützte Netzwerk passieren. Wird diese Verbindung wieder abgebaut, so hat kein System aus dem ungeschützten Netzwerk die Möglichkeit, Pakete in ihrem abgesicherten Netzwerk zu platzieren - es sei denn, Sie wollen es so und erlauben diesen Vorgang explizit.

Anwendungsschicht-Gateways: Application Proxy Firewall (Application Gateway)

Die zweite maßgebende Art von Firewalls sind die Anwendungsschicht-Gateways. Sie nehmen Verbindungen zwischen außenstehenden Systemen und Ihrem Netzwerk stellvertretend an. In diesem Fall werden Pakete nicht weitergeleitet, sondern es findet eine Art Übersetzung statt, mit dem Gateway als Zwischenstation und Übersetzer.

Die Stellvertreterprozesse auf dem Application Gateway werden als **Proxyserver** oder kurz **Proxies** bezeichnet. Jeder *Proxy* kann speziell für den Dienst, für den er zuständig ist, weitere Sicherheitsmerkmale anbieten. Es ergeben sich weitere umfangreiche Sicherungs- und Protokollierungsmöglichkeiten durch die Verwendung von *Proxies*.

Die Analyse ist auf dieser Kommunikationsebene besonders intensiv möglich, da der Kontext der Anwendungsdaten jeweils klar durch Protokollstandards definiert ist. Die Proxies konzentrieren sich auf das Wesentliche. Der Vorteil ist, dass kleine überschaubare Module verwendet werden, wodurch die Fehleranfälligkeit durch Implementationsfehler reduziert wird.

Bekannte Proxies sind z. B.:

- HTTP-Proxy mit Java, JavaScript & ActiveX-Filter
- SMTP-Proxy, verantwortlich für die Zustellung von E-Mails und für das Überprüfen auf vorhandene Viren
- SOCKS-Proxy als generischer, authentifizierungssfähiger Circuit-Level-Proxy

Der Vorteil der Anwendungsschicht-Gateways ist, dass das gesicherte Netzwerk physikalisch und logisch vom ungesicherten Netzwerk getrennt wird. Sie stellen sicher, dass kein Paket direkt zwischen den Netzwerken fließen kann. Direktes Resultat daraus ist ein reduzierter Administrationsaufwand. Sie stellen lediglich die Integrität der Stellvertreter sicher und schützen damit sämtliche Clients und Server in Ihrem Netzwerk - unabhängig von Marke, Programmversion oder Plattform.

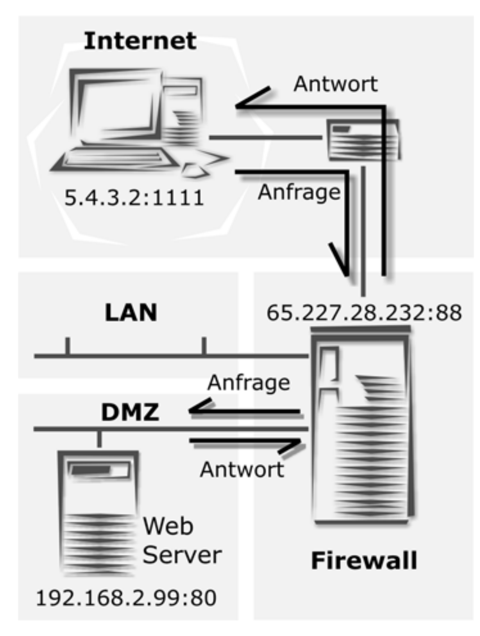
Schutzmechanismen

Weitere Mechanismen gewährleisten zusätzliche Sicherheit:

Die Verwendung privater IP-Adressen in den geschützten Netzwerken, gepaart mit **Network Address Translation (NAT)** in den Ausprägungen ...

- Masquerading
- Source NAT (SNAT)
- Destination NAT (DNAT)

erlaubt es, ein gesamtes Netzwerk hinter einer oder wenigen offiziellen IP-Adressen zu verbergen und die Erkennung Ihrer Netztopologie von außen zu verhindern.



Bei nach wie vor voll verfügbarer Internet-Konnektivität ist nach außen hin keine Identifikation von Endsystemen mehr möglich.

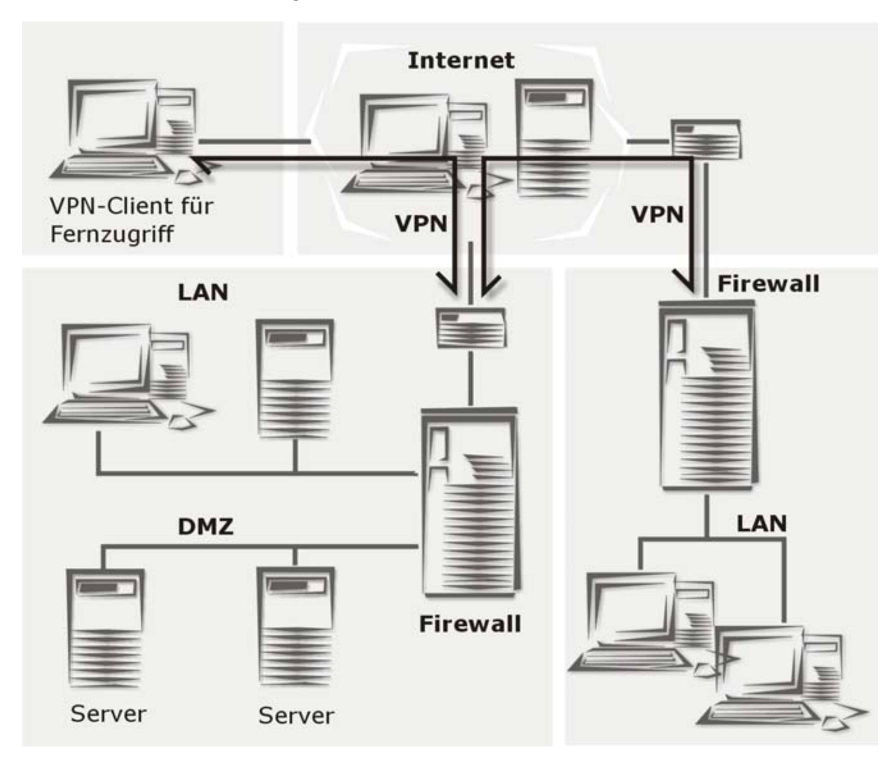
Durch **Destination NAT** ist es allerdings möglich, Server innerhalb des geschützten Netzwerks oder der DMZ zu platzieren und für einen bestimmten Dienst nach außen hin verfügbar zu machen.

Beispiel: Ein Benutzer (wie in der linken Grafik dargestellt) mit der IP-Adresse 5.4.3.2, Port 1111 schickt eine Anfrage an den Web-Server in der DMZ. Er kennt nur die externe IP-Adresse (65.227.28.232, Port 88). Durch **DNAT** ändert nun die Firewall die Zieladresse der Anfrage in 192.168.2.99, Port 80 und schickt diese an den Web-Server. Der Web-Server schickt anschließend die Antwort mit seiner internen IP-Adresse (192.168.2.99, Port: 80) und der IP-Adresse des Benutzers ab. Die Firewall erkennt das Paket anhand der Benutzeradresse und ändert nun die Quelladresse von der internen in die externe IP-Adresse (65.227.28.232, Port 88).

Ein weiterer wichtiger Schutzmechanismus ist die VPN-Technologie. Die Geschäftswelt stellt heute Anforderungen an die IT-Infrastruktur, zu denen Echtzeit-Kommunikation und enge Zusammenarbeit mit Geschäftspartnern, Consultants und Zweigstellen gehören. Die Forderung nach Echtzeitfähigkeit führt immer öfter zur Schöpfung so genannter Extranets, die mit dem Netzwerk des Unternehmens entweder ...

- über dedizierte Standleitungen, oder
- unverschlüsselt über das Internet

... erfolgen. Dabei hat jede dieser Vorgehensweisen Vor- und Nachteile, da ein Konflikt zwischen den entstehenden Kosten und den Sicherheitsanforderungen auftritt.



Durch **Virtual Private Network (VPN)** wird es möglich, abgesicherte, d. h. verschlüsselte Verbindungen zwischen LANs aufzubauen, die transparent von Endpunkt zu Endpunkt über das Internet geleitet werden. Dies ist insbesondere sinnvoll, wenn Ihre Organisation an mehreren Standpunkten operiert, die über eine Internet-Anbindung verfügen. Aufbauend auf dem IPSec-Standard wird es hier möglich, sichere Verbindungen herzustellen.

Unabhängig von der Art der zu übertragenden Daten wird diese verschlüsselte Verbindung automatisch (d. h. ohne die Notwendigkeit zusätzlicher Konfigurationen oder Passwörter am Endsystem) genutzt, um den Inhalt während des Transports abzusichern.

ISO/OSI	TCP/IP
7 Application Layer	Application Level FTP, SMTP/E-mail
6 Presentation Layer	
5 Session Layer	
4 Transport Layer	Transmission Level TCP, UDP
3 Network Layer	Internet Level IP, ICMP
2 Data Link Layer	Network Level Ethernet
1 Physical Layer	

Am anderen Ende der Verbindung werden die übermittelten Daten wieder transparent entschlüsselt und stehen in ihrer ursprünglichen Form dem Empfänger zur Verfügung.

Die **Firewall** dieses Internet-Sicherheitssystems ist ein Hybrid aus den genannten Schutzmechanismen und vereinigt die Vorteile aller Varianten:

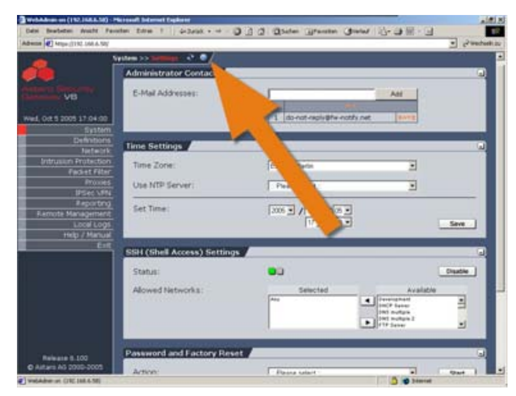
Die **Stateful-Inspection Packet-Filter**-Funktionalität bietet plattformunabhängig die nötige Flexibilität, um alle nötigen Dienste definieren, freischalten oder sperren zu können.

Vorhandene **Proxies** machen dieses Internet-Sicherheitssystem zum **Application Gateway**, der die wichtigsten Endsystemdienste wie **HTTP**, **Mail** und **DNS** durch Stellvertreter absichert und zudem durch SOCKS generisches Circuit-Level-Proxying ermöglicht.

VPN, **SNAT**, **DNAT**, **Masquerading** und die Möglichkeit, **statische Routen** zu definieren, erweitern die dedizierte Firewall zu einem leistungsfähigen Knoten- und Kontrollpunkt in Ihrem Netzwerk.

3. Installation

Die Installation des Internet-Sicherheitssystems gliedert sich in zwei Teile. Der erste Teil beinhaltet das Einspielen der Software - dies führen Sie im **Installationsmenü** durch. Der zweite Teil ist die Konfiguration des Internet-Sicherheitssystems und erfolgt im webbasierten Konfigurationstool **WebAdmin** von Ihrem Arbeitsplatz aus.



Hinweise zur Funktionalität des **WebAdmin** entnehmen Sie der **Online Help**. Die Hilfe wird über die Schaltfläche **?** geöffnet. Die Online Help steht auf englischer Sprache zur Verfügung.

Auf den folgenden Seiten können Sie die Daten zur Konfiguration (z. B. das Default Gateway und die IP-Adressen der installierten Netzwerkkarten) in die entsprechenden Felder eintragen und anschließend archivieren.

Achtung:

Falls Sie Ihr Internet-Sicherheitssystems von **Astaro Security Linux V5** auf **Astaro Security Gateway V6** aktualisieren und die bestehende Konfiguration übernehmen wollen, müssen Sie zuvor Ihr bestehendes System mindestens auf Version 5.200 updaten. Weitere Informationen zum Up2Date-Service und zur Backup-Funktion erhalten Sie in den Kapiteln 5.1.3 und 5.1.4.

3.1. Systemvoraussetzungen

Damit Sie das Sicherheitssystem auf Ihrer Hardware installieren können, müssen die nachfolgenden Voraussetzungen erfüllt sein:

Hardware

- Prozessor: Pentium II oder kompatibel (bis zu 100 Benutzer)
  Prozessor: Pentium III oder kompatibel (über 100 Benutzer)
- 256 MB Arbeitsspeicher
- 8 GB IDE oder SCSI Festplatte
- Bootfähiges IDE oder SCSI CD-ROM-Laufwerk
- 2 oder mehr PCI Ethernet Netzwerkkarten
- 1 USB Port für Kommunikation mit UPS-Gerät (optional).
  Weitere Informationen erhalten Sie auf Seite 22.

Wichtiger Hinweis:

Für das **High Availability (HA)**-System und zur Konfiguration eines **Virtual LAN** benötigen Sie Hardware, die vom Sicherheitssystem für die entsprechende Funktion unterstützt wird. Die **Hardware Compatibility List (HCL)** befindet sich auf **www.astaro.com/kb**. Mit Hilfe des Suchbegriffs **HCL** gelangen Sie schnell auf die entsprechende Seite.

Zur einfacheren Konfiguration des **High Availability (HA)**-Systems mit Überwachung mittels *Heart Beat* empfiehlt es sich für alle Schnittstellen Netzwerkkarten aus der *Hardware Compatibility List (HCL)* zu verwenden. Die Installation des **HA**-Systems wird in Kapitel 5.1.11 ab Seite 122 beschrieben.

UPS-Geräte-Support

Mit einem **UPS**-Gerät (*Uninterruptible Power Supply*, oder **USV** für *Unterbrechungsfreie Stromversorgung*) können Sie sicherstellen, dass bei einem Stromausfall wichtige Geräte nicht unvorhergesehen ausfallen. Das Sicherheitssystem unterstützt ab Version 6.102 die *UPS*-Geräte der Hersteller **MGE UPS Systems** und **APC**. Die Kommunikation zwischen dem *UPS*-Gerät und dem Sicherheitssystem erfolgt über die *USB*-Schnittstelle. Sobald das *UPS*-Gerät im Batteriebetrieb läuft, wird eine **Notification** an den Administrator abgeschickt. Falls der Stromausfall längere Zeit andauert und sich die Spannung des *UPS*-Geräts einem kritischen Wert neigt, erfolgt wiederum eine entsprechende Meldung an den Administrator und das Sicherheitssystem wird automatisch heruntergefahren. Die Ereignisse werden ebenfalls im Menü **Administration** und im **Executiv Report** protokolliert.

Das Menü **Administration** wird in Kapitel 5.8.1 auf Seite 398 beschrieben. Weitere Informationen zum **Executiv Report** erhalten Sie in Kapitel 5.8.12 auf Seite 404. Die Einstellungen für die **Notification E-Mails** werden in Kapitel 5.1.1 ab Seite 48 beschrieben.

Achtung:

Beachten Sie beim Anschließen der Geräte die Betriebsanleitung zum *UPS*-Gerät. Das Sicherheitssystem erkennt das *UPS*-Gerät beim Hochfahren über die *USB*-Schnittstelle. Achten Sie daher darauf, dass Sie das *Sicherheitssystem* erst einschalten, wenn Sie auch die *USB*-Schnittstellen miteinander verbunden haben.

Administrations-PC

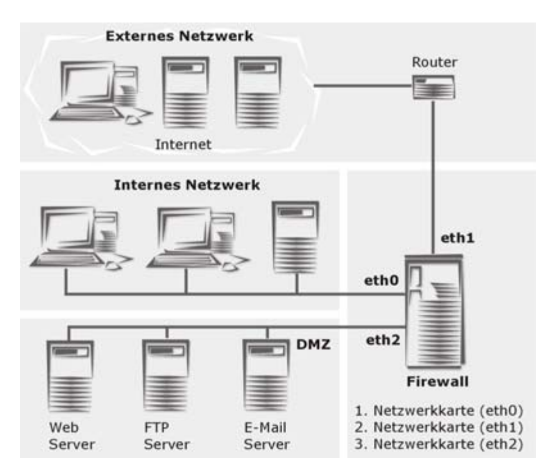
- Korrekte Konfiguration der **IP-Adresse**, der **Subnetzwerkmaske** und des **Default Gateway**.
- Ein HTTPS-fähiger Browser (Microsoft Explorer 5.0 oder höher, Netscape Communicator 6.1 oder höher oder Mozilla 1.6+):

  Im Browser muss **JavaScript** aktiviert sein.

  Im Browser muss die IP-Adresse der **internen Netzwerkkarte (eth0)** auf dem Internet-Sicherheitssystem von der Verwendung eines Proxyservers ausgeschlossen sein!

  Die Konfiguration des Browsers wird in Kapitel 5.6.1 auf Seite 270 beschrieben.

Beispielkonfiguration



Das Internet-Sicherheitssystem sollte, wie in der linken Konfiguration dargestellt, die einzige Verbindung zwischen Ihrem internen (LAN) und dem externen Netzwerk (Internet) herstellen.

Adresstabelle

	IP-Adresse	Netzwerkmaske	Default Gateway
Mit internem Netzwerk verbundene Netzwerk-karte	___.___.___.___	___.___.___.___	___.___.___.___
Mit exter-nem Netz-werk ver-bundene Netzwerk-karte	___.___.___.___	___.___.___.___	___.___.___.___
Mit DMZ verbundene Netzwerk-karte [1]	___.___.___.___	___.___.___.___	___.___.___.___
Netzwerk-karte für HA-System[2]	___.___.___.___	___.___.___.___	

[1] Die dritte und weitere Netzwerkkarten sind optional.

[2] Netzwerkkarte für High Availability (HA).

3.2. Installationsanleitung

Ab hier werden Sie schrittweise durch die Installation geführt.

Achtung:

Bei der Installation der Software werden alle bestehenden Daten auf der Festplatte gelöscht!

Vorbereitung

Bitte legen Sie vor der Installation folgende Unterlagen bereit:

- Internet-Sicherheitssystem CD-ROM
- den **License Key** für das Sicherheitssystem
- die ausgefüllte Adresstabelle mit den **IP-Adressen** und **Netzwerkmasken** sowie die IP-Adresse des **Default Gateway**

3.2.1. Software installieren

Den ersten Teil der Installation führen Sie im Installationsmenü durch.

Zuerst erfolgt ein Hardware-Check. Anschließend geben Sie über den Dialog die Daten ein und danach wird die Software auf Ihrem PC eingespielt.

1. ***PC von der CD-ROM booten:***

   Wählen Sie den passenden Installationsmodus für Ihren Rechner aus. Es stehen drei vorkompilierte Kernel-Varianten zur Auswahl:

   Default: Kernel für Systeme mit einer CPU.

   SMP: Kernel für Systeme mit mehreren Prozessoren.

   Classic: Kernel für Systeme mit einer CPU, wobei die Unterstützung für *APIC* (Advanced Programmable Interrupt Controller)

und *ACPI* (Advanced Configuration and Power Interface) ausgeschaltet ist.

Da bei älteren Hardware-Komponenten oftmals *APIC* und *ACPI* nicht unterstützt werden, empfehlen wir in diesem Fall den **Classic** Kernel zu installieren!

2. *Tastenfunktionen während der Installation (Schritt 1):*

Die Navigation im Installationsmenü erfolgt über die nachfolgenden Tasten. Beachten Sie während der Installation auch die zusätzlichen Tastenfunktionen in der grünen Fußleiste.

Cursor-Tasten: Navigation in den Texten, z. B. in den Lizenzbestimmungen und zur Auswahl des Keyboard-Layouts.

Enter-Taste: Die Eingabe wird bestätigt und zum nächsten Punkt fortgefahren.

ESC-Taste: Abbruch der Installation.

Tab-Taste: Wechseln zwischen den Text- und Eingabefeldern sowie den Schaltflächen.

Klicken Sie auf die **Enter**-Taste.

! **Achtung:**

Bei der Installation der Software werden alle bestehenden Daten auf dem PC gelöscht!

Bestätigen Sie die anschließende Sicherheitsabfrage durch einen Klick auf die **F8**-Taste.

3. *Keyboard-Layout (Schritt 2):*

Wählen Sie mit den **Cursor**-Tasten das Keyboard-Layout aus und bestätigen Sie dies mit der **Enter**-Taste.

4. *Hardware-Erkennung (Schritt 3):*

Die Software prüft die folgenden Hardware-Komponenten: Prozessor, Fabrikat und Größe der Festplatte, CD-ROM-Laufwerk, Netzwerkkarten sowie den IDE- bzw. SCSI-Controller.

Falls die vorhandenen Hardware-Ressourcen zur Installation der Software nicht ausreichen, wird die Installation mit der entsprechenden Fehlermeldung abgebrochen.

5. ***Datum und Uhrzeit (Schritt 4):***

Wählen Sie mit den **Cursor**-Tasten das Land aus und bestätigen Sie dies mit der **Enter**-Taste.

Wählen Sie mit den **Cursor**-Tasten die Zeitzone aus und bestätigen Sie dies mit der **Enter**-Taste.

Tragen Sie anschließend in die Eingabefelder das aktuelle Datum und die Uhrzeit ein. Sie können mit der **Tab**-Taste und den **Cursor**-Tasten zwischen den Eingabefeldern wechseln. Ungültige Eingaben werden nicht übernommen.
Bestätigen Sie die Eingaben mit der **Enter**-Taste.

6. ***Netzwerkkarte auswählen und konfigurieren (Schritt 5):***

Damit Sie nach der Software-Installation das Internet-Sicherheitssystem mit dem Tool **WebAdmin** konfigurieren können, müssen Sie eine Netzwerkkarte definieren. Diese Netzwerkkarte ist später die **interne Netzwerkkarte (eth0)**.
Wählen Sie aus den verfügbaren Netzwerkkarten eine aus und bestätigen Sie die Auswahl mit der **Enter**-Taste.

Definieren Sie anschließend für diese Netzwerkkarte die **IP-Adresse**, die **Netzwerkmaske** und das **Gateway** (Default Gateway).

Beispiel:

Address: 192.168.2.100

Netmask: 255.255.255.0

Den **Gateway** müssen Sie eingeben, wenn Sie mit einem PC auf das Konfigurationstool **WebAdmin** zugreifen möchten, der außerhalb des Netzwerkbereichs liegt. Beachten Sie dabei, dass das Gateway innerhalb des Netzwerkbereichs liegen muss.

Bei der Netzwerkmaske 255.255.255.0, wird das Sub-Netzwerk durch die ersten drei Werte definiert. In unserem Beispiel lautet der relevante Bereich 192.168.2. Wenn nun Ihr Administrations-PC z. B. die IP-Adresse 192.168.10.5 hat, liegt er nicht im selben Sub-Netzwerk und in diesem Fall benötigen Sie ein Gateway. Für unser Beispiel nehmen wird die folgende Adresse:

Gateway: 192.168.2.1

Falls der Administrations-PC innerhalb des Netzwerkbereichs liegt, geben Sie den folgenden Wert ein:

Gateway: none

Bestätigen Sie die Eingaben mit der **Enter**-Taste.

7. ***Lizenzbestimmungen (Schritt 6):***

Hinweis:

Beachten Sie die rechtlichen Hinweise und Lizenzbestimmungen.

Die Lizenzbestimmungen akzeptieren Sie mit der **F8**-Taste.

8. ***Abschließende Hinweise (Schritt 7):***

Achtung:

Beachten Sie die abschließenden Hinweise zur Installation der Software. Nach Bestätigung des Warnhinweises werden alle bestehenden Daten auf dem PC gelöscht!

Falls Sie Eingaben ändern möchten, können Sie nun mit der **F12**-Taste wieder zu Schritt 1 des Installationsmenüs gelangen.

Sie starten die Installation der Software mit der **F8**-Taste.

9. ***Software installieren (Schritt 8):***

Die Installation der Software kann nun einige Minuten dauern. Sie können den Installationsvorgang mit Hilfe von vier Konsolen verfolgen.

Die vier Konsolen:

Install-Routine: (**Alt** + **F1**).

Interaktive **Bash**-Shell (**Alt** + **F2**).

Log-Ausgabe der Install-Routine (**Alt** + **F3**).

Kernel-Ausgabe (**Alt** + **F4**).

Sobald Sie dazu aufgefordert werden, entnehmen Sie die CD-ROM aus dem Laufwerk und verbinden die Netzwerkkarte **eth0** mit Ihrem lokalen Netzwerk.

Mit Ausnahme der **internen Netzwerkkarte (eth0)** wird die Reihenfolge der Netzwerkkarten in erster Linie durch die **PCI ID** und den **Kernel**-Treiber bestimmt.

Die Reihenfolge der Netzwerkkartenbenennung kann sich auch später durch Änderung der Hardwarekonfiguration, z. B. durch das Hinzufügen oder Entfernen von Netzwerkkarten und der damit verbundenen Neuinstallation ändern.

10. Internet-Sicherheitssystem neu starten:

Starten Sie das Internet-Sicherheitssystem mit der Tastenkombination **Strg** + **Alt** + **Entf** oder durch **Reset** neu.

Während des Boot-Vorgangs wird die IP-Adresse der internen Netzwerkkarte neu gesetzt, daher kann auf der Konsole **Install-Routine** (**Alt** + **F1**) für kurze Zeit die Meldung `No IP on eth0` angezeigt werden.

Nachdem das Internet-Sicherheitssystem neu gestartet ist (je nach Hardware dauert dies bis zu fünf Minuten), sollten Sie mittels **Ping** die IP-Adresse der **eth0**-Netzwerkkarte erreichen.

Falls keine Verbindung zustande kommt, prüfen Sie bitte Ihr System auf die nachfolgenden möglichen Fehlerquellen.

Fehler:

Sie erreichen das Internet-Sicherheitssystem nicht vom lokalen Netzwerk.

Mögliche Fehlerursachen:



- IP-Adresse des Internet-Sicherheitssystems ist nicht korrekt gesetzt
- IP-Adresse am Client-Rechner ist nicht korrekt gesetzt
- Default Gateway am Client-Rechner ist nicht korrekt gesetzt
- Netzwerkkabel ist mit der falschen Netzwerkkarte verbunden
- Alle Netzwerkkarten des Internet-Sicherheitssystems sind an einem Hub angeschlossen

Hinweis:

Falls Sie für Ihre Verbindung zum Internet **DSL** verwenden, beachten Sie bei der Konfiguration den entsprechenden Leitfaden unter der Internetadresse **http://www.astaro.com/kb**.

3.2.2. Sicherheitssystem konfigurieren

Die Konfiguration des Sicherheitssystems führen Sie von Ihrem Administrations-PC aus mit einem Internet Browser (z. B. MS Internet Explorer) und dem Konfigurationstool **WebAdmin** durch:

1. ***Browser starten und WebAdmin öffnen:***

Bevor Sie das Konfigurationstool **WebAdmin** öffnen können, müssen Sie den Browser entsprechend konfigurieren. Weitere Informationen erhalten Sie in Kapitel 5.6.1 ab Seite 269.

Wenn der Browser konfiguriert ist, geben Sie die IP-Adresse des Internet-Sicherheitssystems (eth0) wie folgt ein: **https://IP-Adresse** (Beispiel aus Install/Schritt 6: https://192.168.2.100).

Anschließend erscheint ein **Sicherheitshinweis**. Dieser Hinweis wird später nicht mehr angezeigt, wenn Sie für Ihre **WebAdmin**-Seite ein Zertifikat generieren.

Ausführliche Informationen zum Zertifikat und wie Sie dieses Zertifikat installieren, wird in Kapitel 5.1.10 ab Seite 119 beschrieben.

Bestätigen Sie die Frage auf dem **Sicherheitshinweis**, ob der Vorgang fortgesetzt werden soll, mit einem Klick auf die Schaltfläche **Ja**.

Beim ersten Start des **WebAdmin** öffnet sich ein Menü mit den Fenstern **License Agreement** und **Setting System Passwords**.

2. ***Lizenzbestimmungen akzeptieren:***

Die Lizenzbestimmungen im Fenster **License Agreement** akzeptieren Sie durch einen Klick auf das Optionsfeld **I agree to the terms of the license**.

Hinweis:

Beachten Sie die rechtlichen Hinweise und Lizenzbestimmungen.

3. ***Passwörter setzen:***

Setzen Sie im Fenster **Setting System Passwords** die Passwörter für das Internet-Sicherheitssystem.



Sicherheitshinweis:

Setzen Sie sichere Passwörter! Ihr Vorname rückwärts buchstabiert ist beispielsweise kein ausreichend sicheres Passwort – besser wäre z. B. xfT35!4z.

Zusammensetzung des Passworts:

Um die Sicherheit für das Sicherheitssystem und somit auch für das interne Netzwerk zu erhöhen unterliegt die Zusammensetzung und die Länge des Passworts den nachfolgend aufgeführten Restriktionen. Das Passwort wird vom Sicherheitssystem nur übernommen, wenn diese Bestimmungen erfüllt sind:

- eine Mindestlänge von acht Zeichen
- mindestens ein kleingeschriebener Buchstabe
- mindestens ein großgeschriebener Buchstabe
- mindestens eine Zahl
- mindestens ein nicht-alphanumerisches Zeichen (innerhalb der ASII-Tabelle, Zeile 32 bis 126)

Sie können **WebAdmin** nur starten, wenn Sie für die folgenden Funktionen ein Passwort gesetzt haben. Bestätigen Sie die Passwörter durch die nochmalige Eingabe in das jeweilige Eingabefeld **Confirm**. Die Benutzernamen (**Username**) sind vorgegeben und können nicht geändert werden.

WebAdmin User: Zugang zum WebAdmin.
Der Benutzername lautet **admin**.

Shell Login User: Zugang via SSH.
Der Benutzername lautet **loginuser**.

Shell Administrator User: Administratorrechte für das gesamte Internet-Sicherheitssystem.
Der Benutzername lautet **root**.



Sicherheitshinweis:

Setzen Sie für **Shell Login** und **Shell Administrator** unterschiedliche Passwörter.

Astaro Configuration Manager User (optional): Dieses Passwort benötigen Sie, falls das Internet-Sicherheitssystem mit dem *Astaro Configuration Manager* konfiguriert werden soll.

Boot Manager (optional): Dieses Passwort verhindert, dass Unbefugte Änderungen in den Bootparametern vornehmen können.

Bestätigen Sie die gesetzten Passwörter durch einen Klick auf die Schaltfläche **Save**.

4. ***Im Konfigurationstool WebAdmin authentifizieren:***

User: **admin**

Password: Passwort des WebAdmin-Benutzers

Beachten Sie bitte die Groß- und Kleinschreibung!

Klicken Sie auf die Schaltfläche **Login**.

Hinweis:

Gehen Sie die Schritte 5 bis 16 in der angegebenen Reihenfolge durch.

---

5. ***License Key einspielen:***

Öffnen Sie im Verzeichnis **System** das Menü **Licensing** und spielen Sie im Fenster **License File** die **Lizenzdatei** (**License Key**) ein.

Hinweis:

Bei einer Lizenz mit der Option **High Availability (HA)** müssen Sie den **License Key** auf beiden Sicherheitssystemen (Normal- und Hot-Standby-Modus) einspielen.

Weitere Informationen zur **Lizenzierung** erhalten Sie in Kapitel 5.1.2 ab Seite 56.

6. ***Erste Grundeinstellungen durchführen:***

Öffnen Sie im Verzeichnis **System** das Menü **Settings** und führen Sie die folgende Einstellungen durch:

Administrator Contact: Tragen Sie in das Hierarchiefeld die E-Mail-Adresse des Administrators ein.

Weitere Informationen zu diesen Funktionen erhalten Sie in Kapitel 5.1.1 ab Seite 48.

Öffnen Sie im Verzeichnis **Network** das Menü **Hostname / Dyn-DNS** und führen Sie die folgende Einstellungen durch:

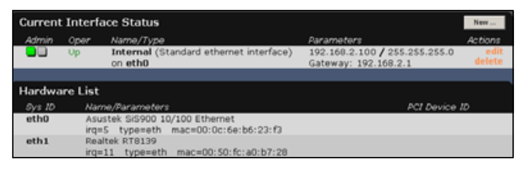
Hostname: Tragen Sie hier den **Hostnamen** für Ihr Internet-Sicherheitssystem ein.
Ein Domainname darf aus alphanumerischen Zeichen sowie Punkt- und Minus-Zeichen bestehen. Am Ende muss ein alphabetischer Bezeichner vorhanden sein, z. B. „com“, „de“ oder „org“. Der **Hostname** wird in allen **Notification E-Mails** in der Betreffzeile angezeigt.

Speichern Sie abschließend die Eingaben durch einen Klick auf die Schaltfläche **Save**.

7. *Interne Netzwerkkarte (eth0) editieren:*

Öffnen Sie im Verzeichnis **Network** das Menü **Interfaces** und prüfen Sie die Einstellungen der **Netzwerkkarte eth0**.

Die Netzwerkkarte (eth0) zum internen Netzwerk wurde von Ihnen während der Installation der Software definiert. Diese Netzwerkkarte wird nach dem ersten Start des Internet-Sicherheitssystems im Fenster **Current Interface Status** angezeigt.



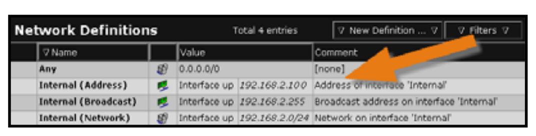
Falls Sie bei dieser Netzwerkkarte Einstellungen ändern möchten, z. B. einen anderen Namen, führen Sie diese jetzt durch. Um die Einstellungen zu editieren öffnen Sie das Menü **Edit Interface** durch einen Klick auf die Schaltfläche **edit**.

Achtung:

Wenn Sie die **IP-Adresse** der internen Netzwerkkarte **eth0** ändern, geht die Verbindung zum **WebAdmin** verloren.

Die Konfiguration der Netzwerkarten und virtuellen Schnittstellen (**Interfaces**) wird in Kapitel 5.3.2 ab Seite 154 beschrieben.

8. Internes Netzwerk konfigurieren:



Öffnen Sie im Verzeichnis **Definitions** das Menü **Networks** und prüfen Sie die Einstellungen für das interne Netzwerk. Während der Installation wurden vom Internet-Sicherheitssystem aufgrund Ihrer Definition der internen Netzwerkkarte (eth0) automatisch drei logische Netzwerke definiert:

Die Schnittstelle **Internal (Address)**, bestehend aus der von Ihnen definierten IP-Adresse (Beispiel: 192.168.2.100) und der Netzwerkmaske 255.255.255.255 (Host).

Der Broadcast **Internal (Broadcast)**, bestehend aus der Broadcast-IP (Beispiel: 192.168.2.255) und der Netzwerkmaske 255.255.255.255 (Host).

Das interne Netzwerk **Internal (Network)**, bestehend aus der Netzwerk-IP-Adresse (Beispiel: 192.168.2.0) und der Netzwerkmaske (Beispiel: 255.255.255.0).

Das Definieren neuer Netzwerke (**Networks**) wird im Handbuch in Kapitel 5.2.1 ab Seite 134 beschrieben.

9. Externe Netzwerkkarte konfigurieren:

Öffnen Sie im Verzeichnis **Network** das Menü **Interfaces** und konfigurieren Sie die Schnittstelle zum externen Netzwerk (Internet). Die Wahl der Schnittstelle und die dafür notwendigen Einstellungen auf der externen Netzwerkkarte hängen von der Art des Internetzugangs ab.

Die Konfiguration der Netzwerkarten und virtuellen Schnittstellen (**Interfaces**) wird in Kapitel 5.3.2 ab Seite 154 beschrieben.

10. *Masquerading-Regel für das interne Netzwerk definieren:*

Falls Sie in Ihrem Netzwerk private IP-Adressen verwenden möchten und eine direkte Verbindung ohne Proxy benötigen, setzen Sie unter dem Verzeichnis **Network** im Menü **NAT** die entsprechenden **Masquerading**-Regeln.

Weitere Informationen zu **DNAT**, **SNAT** und **Masquerading** erhalten Sie im Kapitel 5.3.5 ab Seite 198.

Die IP-Routing-Einträge für an die Netzwerkkarten angeschlossene Netzwerke (**Interface Routes**) werden automatisch erstellt. Bei Bedarf können Sie im Menü **Routing** IP-Routing-Einträge auch manuell definieren. Dies ist allerdings nur in komplexeren Netzwerken notwendig.

11. *DNS-Proxy konfigurieren:*

Öffnen Sie im Verzeichnis **Proxies** das Menü **DNS** und konfigurieren Sie den DNS-Proxy.

Durch die Konfiguration des DNS-Proxy beschleunigen Sie die Namensauflösung. Sie können einen lokalen **Nameserver (DNS)** oder den Ihres Internet Service Providers eintragen. Andernfalls verwendet Ihr Internet-Sicherheitssystem automatisch die **Root-Nameserver**.

Die Konfiguration des **DNS-Proxy** wird in Kapitel 5.6.4 ab Seite 336 beschrieben.

12. *Weitere Netzwerke anschließen:*

Falls noch weitere interne Netzwerke vorhanden sind, verbinden Sie diese mit den Netzwerkkarten des Internet-Sicherheitssystems.

13. *HTTP-Proxy konfigurieren:*

Falls Rechner im internen Netzwerk unter Verwendung des Proxies auf das Internet zugreifen sollen, öffnen Sie im Verzeichnis **Proxies** das Menü **HTTP** und schalten Sie den Proxy durch einen Klick auf die Schaltfläche **Enable** ein.

Damit die Rechner im internen Netzwerk anschließend unter Verwendung des HTTP-Proxy auf das Internet zugreifen können, müssen die Browser eventuell konfiguriert werden - z. B. wenn der Proxy für den Betriebsmodus Standard konfiguriert wurde.

Die Konfiguration des **HTTP-Proxy** wird in Kapitel 5.6.1 ab Seite 269 beschrieben.

14. *Die Paketfilterregeln setzen:*

Öffnen Sie im Verzeichnis **Packet Filter** das Menü **Rules** und setzen Sie die Paketfilterregeln.

Neue Regeln werden inaktiv an letzter Stelle angefügt und müssen dann einsortiert werden. Die Regeln werden von oben nach unten abgearbeitet, wobei die Verarbeitung durch die erste zutreffende Regel beendet wird. Durch einen Klick auf die Statusampel wird die Regel aktiv (Statusampel zeigt Grün).
Beachten Sie, dass aufgrund von **Stateful Inspection** nur für den Verbindungsaufbau Paketfilterregeln gesetzt werden müssen. Die Antwort- oder Rückpakete werden automatisch erkannt und akzeptiert.
Das Setzen von Paketfilterregeln (**Packet Filter**) wird in Kapitel 5.5 ab Seite 243 beschrieben.

15. *Paketfilter beobachten / Debugging:*

Mit der Funktion **Packet Filter Live Log** im Menü **Packet Filter / Advanced** können Sie sehen, welche Datenpakete in Ihrem Paketfilter gefiltert werden. Wenn nach der Installation des Internet-Sicherheitssystems Probleme auftauchen, so eignen

sich diese Informationen zum **Debugging** Ihrer Paketfilterregeln.

Die Funktion **Packet Filter Live Log** wird in Kapitel 5.5.3 ab Seite 260 beschrieben.

16. ***Sicherheitssystem und Virenscanner aktualisieren:***

Öffnen Sie im Verzeichnis **System** das Menü **Up2Date Service** und führen Sie das **System Up2Date** aus.

Falls Ihre Lizenz auch **Virus Protection** beinhaltet, starten Sie anschließend manuell die Funktion **Pattern Up2Date**.

Das Modul **Up2Date Service** wird in Kapitel 5.1.3 ab Seite 60 beschrieben.

Wenn Sie diese Schritte erfolgreich durchgeführt haben, ist die Erstkonfiguration des Internet-Sicherheitssystems abgeschlossen. Schließen Sie nun das Konfigurationstool **WebAdmin** durch einen Klick auf die Schaltfläche **Exit**.

Probleme

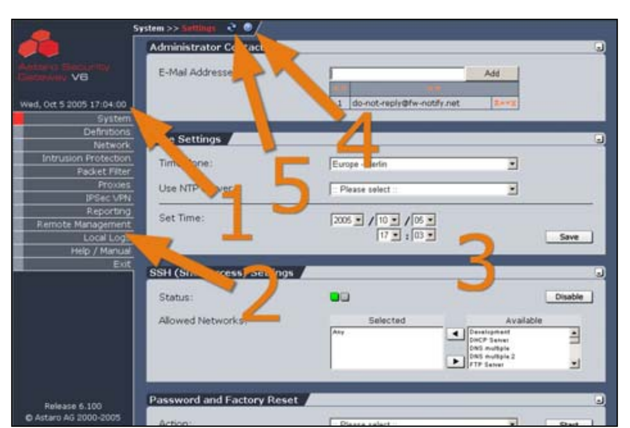
Sollten bei der Durchführung dieser Schritte Probleme auftauchen, so wenden Sie sich bitte an den Support ihres Sicherheitssystem-Anbieters, oder besuchen Sie das **Astaro Bulletin Board** unter:

http://www.astaro.org

4. WebAdmin-Werkzeuge

Mit dem Konfigurationstool **WebAdmin** können Sie alle Einstellungen am Internet-Sicherheitssystem durchführen. In diesem Kapitel werden die Werkzeuge und Hilfsmittel von WebAdmin erläutert.

Das Konfigurationstool **WebAdmin** besteht aus fünf Komponenten:



(1) Info-Box

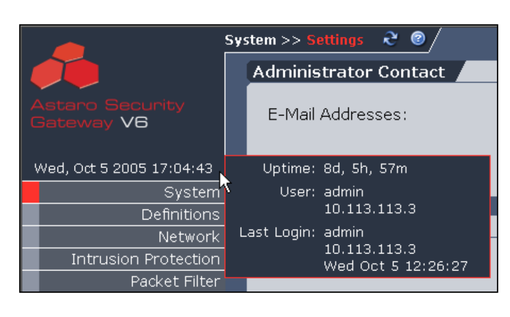
(2) Verzeichnis

(3) Menü

(4) Online-Hilfe

(5) Refresh

4.1. Info-Box



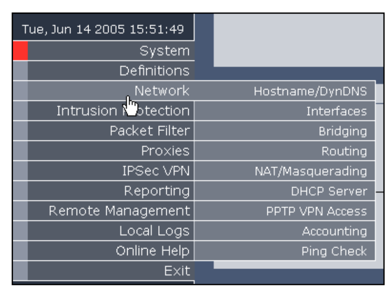
In der linken oberen Ecke wird die die Systemzeit und die Zeitzone angezeigt. Die hinterlegte Info-Box wird geöffnet, wenn Sie mit der Maus die Zeitangabe berühren. Folgende Informationen werden angezeigt:

Uptime: Dokumentiert die Verfügbarkeit Ihres Internet-Sicherheitssystems, d. h. den Zeitraum seit dem das System ohne Unterbrechung verfügbar ist.

User: Zeigt an, welcher Benutzer von welchem Client aus gerade auf den **WebAdmin** zugreift.

Last Login: Zeigt an, wann und von welchem Client aus das letzte Mal auf den **WebAdmin** zugegriffen wurde.

4.2. Das Verzeichnis

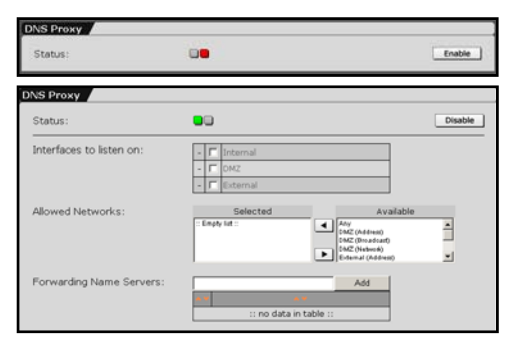


Über das Verzeichnis gelangen Sie in die einzelnen Menüs, um das Internet-Sicherheitssystem zu administrieren. Damit Sie im Handbuch die entsprechende Funktionsbeschreibung schnell finden, entspricht das Kapitel 5 „System benutzen & beobachten“ der Verzeichnisstruktur des **WebAdmin**.

4.3. Menü

Für jede Funktion des Internet-Sicherheitssystems ist im Konfigurationstool **WebAdmin** ein separates Menü enthalten. Diese Menüs enthalten hilfreiche Werkzeuge, die in diesem Kapitel erklärt werden.

4.3.1. Die Statusampel



Einige Funktionen des Internet-Sicherheitssystems sind nach der Installation per Default-Einstellung ausgeschaltet, da diese zuerst konfiguriert werden müssen.

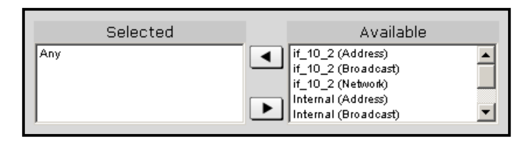
Der aktuelle Status einer Funktion wird durch die Sta-

tusampel angezeigt:

- rot = Funktion ist ausgeschaltet
- grün = Funktion ist eingeschaltet

Die Werkzeuge zur Konfiguration dieser Funktionen und Dienste werden erst geöffnet, wenn die Statusampel Grün zeigt.

4.3.2. Das Auswahlfeld



Mit dem **Auswahlfeld** werden den Funktionen und Diensten die dafür **befugten Netzwerke** (Allowed Networks) und **Benutzer** (Allowed Users) zugeordnet.

Netzwerk oder Benutzer zuordnen:

1. Wählen Sie im Feld **Available** das Netzwerk bzw. den Benutzer aus, indem Sie den entsprechenden Namen mit der Maus markieren.

   Sie können mehrere Namen auf einmal auswählen, indem Sie die **CTRL**-Taste während der Auswahl gedrückt halten.

2. Klicken Sie auf die Schaltfläche **Pfeil nach links**.

   Der Name wird nun in das Feld **Selected** verschoben.

Netzwerk oder Benutzer entnehmen:

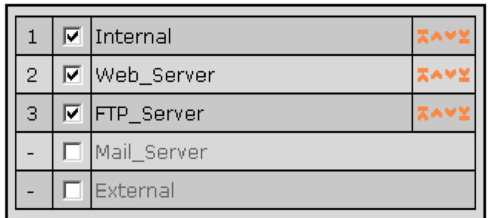
1. Wählen Sie im Feld **Selected** das Netzwerk bzw. den Benutzer aus, indem Sie den entsprechenden Namen mit der Maus markieren.

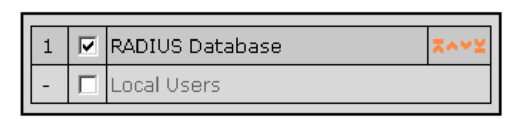
   Sie können mehrere Namen auf einmal auswählen, indem Sie die **CTRL**-Taste während dem Markieren gedrückt halten.

2. Klicken Sie auf die Schaltfläche **Pfeil nach rechts**.

   Der Name wird nun in das Feld **Available** verschoben.

4.3.3. Die Auswahltabelle





Mit der **Auswahltabelle** wird den Funktionen und Diensten die entsprechende **Authentifizierungsmethode** oder eine **Netzwerkkarte** (Interface) zugewiesen.

Die Authentifizierungsmethode (Menü **System / User Authentication**) und die Netzwerkkarten (Menü **Network / Interfaces**) müssen vom Administrator zuerst konfiguriert werden. Das obere Bild zeigt eine Auswahltabelle für Schnittstellen. Das untere Bild enthält eine Tabelle zur Auswahl der Authentisierung.

Die Funktionen zu den Einträgen:

Die Funktionen werden erst aktiviert, wenn der betreffende Eintrag ausgewählt wurde. In der linken Spalte wird die Position des Eintrags angezeigt. Mit den Schaltflächen in der rechten Spalte wird die Reihenfolge der Einträge verändert. Durch einen Klick auf die Schaltflächen oder wird der jeweilige Eintrag um eine Zeile nach vorne bzw. nach hinten verschoben.
Durch einen Klick auf die Schaltfläche oder wird der jeweilige Eintrag in die erste bzw. in die letzte Zeile der Tabelle verschoben.

Authentifizierungsmethode oder Netzwerkkarte zuordnen:

Wählen Sie die Authentifizierungsmethode bzw. die Netzwerkkarte durch einen Klick auf das Kontrollkästchen aus.

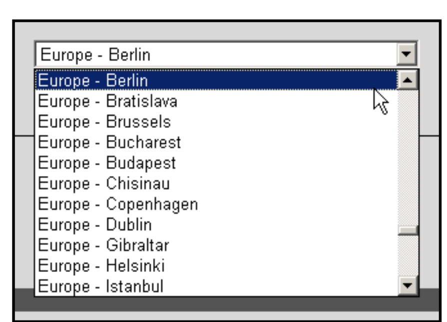
Anschließend wird die neue Einstellung aktiviert und in die letzte Zeile der bereits ausgewählten Einträge verschoben.

Authentifizierungsmethode oder Netzwerkkarte ausschalten:

Der Eintrag wird ausgeschaltet, indem Sie in der entsprechenden Zeile auf das aktivierte Kontrollkästchen klicken.

Der Eintrag wird sofort deaktiviert. Die Funktionen in dieser Zeile stehen dann nicht mehr zur Verfügung.

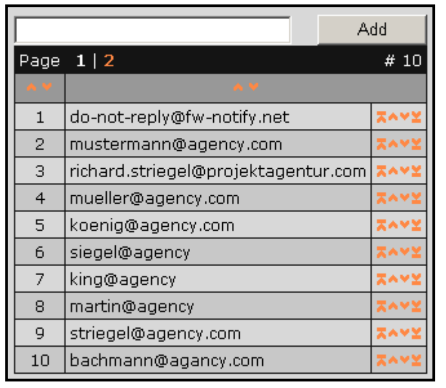
4.3.4. Das Drop-down-Menü



Das **Drop-down-Menü** wird bei Funktionen verwendet, für die immer nur ein bestimmter Wert eingestellt werden kann.

Bei den Drop-down-Menüs werden die ausgewählten Werte in der Regel sofort vom System übernommen.

4.3.5. Das Hierarchiefeld



Das **Hierarchiefeld** kommt bei Funktionen zum Einsatz, bei denen mehrere E-Mail- oder IP-Adressen zugewiesen werden können. Im Hierarchiefeld werden pro Seite 10 Einträge dargestellt.



In der ersten Zeile wird die Anzahl der Seiten (Page) und der Einträge (#) angezeigt. Die aktuelle Seitenzahl ist weiß dargestellt. Wenn Sie mit der Maus die roten Seitenzahlen berühren, werden in einer Info-Box die darin enthaltenen Intervalle angezeigt (kleines Bild).

Mit den Pfeilen in der zweiten Zeile kann die Reihenfolge der Einträge verändert werden. Die hier durchgeführten Einstellungen haben allerdings keinen Einfluss auf die Funktionalität: Mit den Schaltflächen und in der linken Spalte werden die Einträge in der Tabelle numerisch auf- bzw. absteigend dargestellt. Mit den Schaltflächen und in der mittleren Spalte werden die Einträge alphanumerisch auf- bzw. absteigend dargestellt.

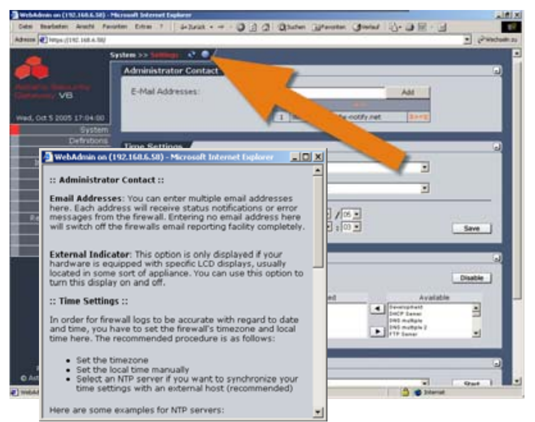
Die funktionale Reihenfolge der Einträge wird mit den Schaltflächen in der rechten Spalte verändert. Durch einen Klick auf die Schaltflächen oder wird der jeweilige Eintrag um eine Zeile nach vorne bzw. nach hinten verschoben.
Durch einen Klick auf die Schaltfläche oder wird der jeweilige Eintrag in die erste bzw. in die letzte Zeile der Tabelle verschoben.

Eintrag hinzufügen: Schreiben Sie die neue Adresse in das Eingabefeld und klicken Sie auf die Schaltfläche **Add**.
Die neue Adresse wird anschließend in die letzte Zeile der Tabelle eingefügt.

Eintrag löschen: Durch einen Doppelklick auf die entsprechende Adresse wird diese sofort aus der Tabelle gelöscht.

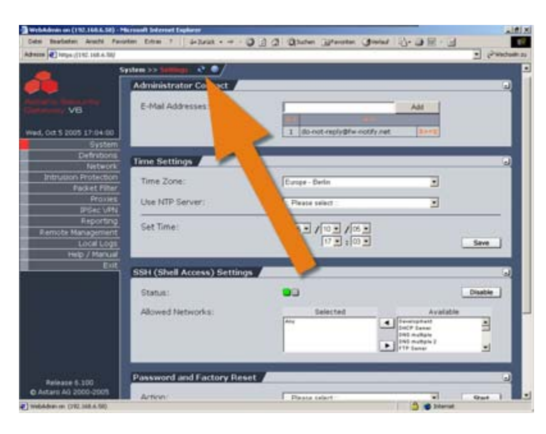
Eintrag bearbeiten: Durch einen Klick auf die entsprechende Adresse, wird diese in das Eingabefeld geladen. Der Eintrag kann nun im Eingabefeld bearbeitet werden.
Durch einen Klick auf die Schaltfläche **Replace** wird der alte Eintrag ersetzt.

4.4. Online-Hilfe



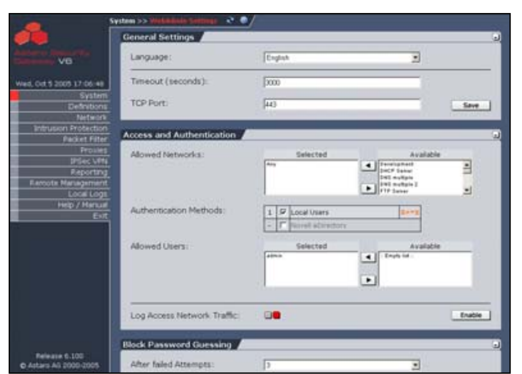
Jedes Menü im Konfigurationstool **WebAdmin** enthält eine **Online-Hilfe** (Online Help), in der die Funktionen kurz erläutert werden. Die Hilfe ist in englischer Sprache verfügbar. Die Hilfe wird durch einen Klick auf die Schaltfläche **?** geöffnet.

4.5. Refresh



Durch einen Klick auf die Schaltfläche **Refresh** wird das Menü neu geladen. Verwenden Sie für die Aktualisierung des Menüs nicht die Schaltfläche **Aktualisieren** in der Werkzeugleiste Ihres Browsers – Sie werden sonst aus der Session geworfen und müssen sich im Konfigurationstool **WebAdmin** neu anmelden!

5. System benutzen & beobachten



WebAdmin ist das webbasierte Konfigurationstool, das Sie bereits von der Installation her kennen.

In diesem Kapitel werden ausführlich die Bedienung des Sicherheitssystems und seine Funktionen beschrieben. Die verschiedenen Einstellungen werden anhand von Step-by-step-Anleitungen erläutert. Dabei wird allerdings nicht auf die Funktionsweise der Werkzeuge eingegangen. Die Werkzeuge werden in Kapitel 4 beschrieben.

Das Ziel des Administrators sollte sein, so wenig wie möglich und so viel wie nötig durch das Sicherheitssystem zu lassen. Dies gilt sowohl für eingehende als auch für ausgehende Verbindungen.

Tipp:

Planen Sie zuerst Ihr Netzwerk und überlegen Sie sich genau welchen Rechnern welche **Dienste (Services)** zugeordnet werden sollen. Dies vereinfacht Ihnen die Konfiguration und erspart Ihnen viel Zeit, die Sie sonst für die nachträgliche Definition von Netzwerken oder Diensten benötigen.

Gehen Sie bei der Konfiguration des Internet-Sicherheitssystems und Ihres Netzwerks folgendermaßen vor:

1. Richten Sie alle erforderlichen Netzwerke und Hosts ein.

2. Definieren Sie die benötigten Dienste auf dem Internet-Sicherheitssystem.

3. Führen Sie nun die Definition Ihres Gesamtsystems durch.

WebAdmin starten:

1. Starten Sie Ihren Browser und geben die IP-Adresse des Internet-Sicherheitssystems (eth0) wie folgt ein: https://IP-Adresse. (Beispiel aus Kapitel 3.2 Installationsanleitung, Schritt 6: https://192.168.2.100)

   Falls Sie noch kein **Zertifikat** für Ihre **WebAdmin**-Seite generiert haben, erscheint ein **Sicherheitshinweis**.
   Ausführliche Informationen zum Zertifikat und wie Sie dieses installieren, finden Sie in Kapitel 5.1.10 ab Seite 119.

2. Bestätigen Sie die Frage auf dem Sicherheitshinweis, ob der Vorgang fortgesetzt werden soll, mit einem Klick auf die Schaltfläche **Ja**.

3. Authentifizieren Sie sich im **WebAdmin**.



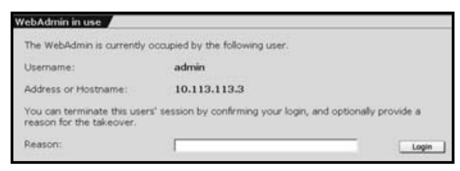
User: **admin**

Password: Passwort des WebAdmin-Benutzers

Beachten Sie bitte die Groß- und Kleinschreibung!

4. Klicken Sie auf die Schaltfläche **Login**.

Ein anderer Administrator ist schon eingeloggt:



Sollte bereits ein anderer Administrator im Konfigurationstool **WebAdmin** angemeldet sein, wird eine entsprechende Meldung angezeigt. Anhand der IP-Adresse können Sie sehen, von welchem Rechner auf das Internet-Sicherheitssystems zugegriffen wird.

Sie können diese Session beenden!

Geben Sie im Eingabefeld **Reason** den Grund für die Übernahme an und klicken anschließend auf die Schaltfläche **Login**.

Nun sind Sie im Internet-Sicherheitssystem eingeloggt und können über das Konfigurationstool **WebAdmin** das System bedienen und beobachten.

5.1. Grundeinstellungen (System)

Im Verzeichnis **System** führen Sie die Grundeinstellungen des Internet-Sicherheitssystems durch.

5.1.1. Settings

Administrator Contact



E-Mail Addresses: Bei wichtigen Ereignissen, z. B. auftretenden Portscans, Anmeldungen mit falschem Passwort, Meldungen des Selfmonitors, bei Up2Date-Prozessen oder bei einem Neustart, werden die Administratoren über die im Hierarchiefeld eingetragenen Adressen benachrichtigt. Es sollte mindestens eine E-Mail-Adresse eingetragen sein. Falls keine Adresse im Hierarchiefeld eingetragen ist, wird die komplette Funktion **Reporting per E-Mail** ausgeschaltet.
Neue E-Mail-Adressen werden vom Eingabefeld durch einen Klick auf die Schaltfläche **Add** in das Hierarchiefeld übernommen.

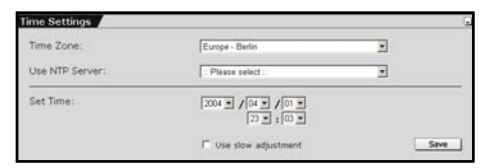
Die Funktionsweise des **Hierarchiefeldes** wird in Kapitel 4.3.5 ab Seite 43 beschrieben.

Wichtiger Hinweis:

An die E-Mail-Adresse des Administrators können **Notification E-Mails** nur zugestellt werden, wenn zuvor der DNS-Proxy (Kapitel 5.6.4 ab Seite 336) eingeschaltet und konfiguriert wurde oder wenn im Menü **SMTP** (Kapitel 5.6.2 ab Seite 304) die Route für eingehende E-Mails definiert wurde.

Use external Indicators: Dieser Schalter wird nur angzeigt, wenn das Internet-Sicherheitssystem auf einer Appliance mit LCD-Anzeige läuft. Mit diesem Schalter können Sie die LCD-Anzeige ein- und ausschalten.

Time Settings



Über dieses Menü stellen Sie das aktuelle Datum und die Uhrzeit des Internet-Sicherheitssystems ein. Sie können die Uhrzeit und das Datum mit Hilfe der Drop-down-Menüs manuell einstellen oder täglich mit einem NTP-Server (Network Time Protocol) synchronisieren. Beachten Sie, dass große Zeitsprünge zu Lücken im **Reporting** und im **Logging** führen.

Wichtiger Hinweis:

Führen Sie keine Umstellung von Winterzeit auf Sommerzeit durch. Tragen Sie am Besten die Central European Time (CET) ein. Während der Sommerzeit entspricht dies einer Abweichung von minus einer Stunde.

Durch Verstellen der Systemzeit kann es zu folgenden zeitsprungbedingten Effekten kommen:

Uhrzeit vorstellen (Winter- auf Sommerzeit)

- Der Time-out für den **WebAdmin** ist abgelaufen und Ihre Session ist nicht mehr gültig.

  In den zeitbasierten Reports fehlen für die entsprechende Zeitspanne die Log-Daten. Die meisten Diagramme stellen diese Zeitspanne als gerade Linie in Höhe des alten Wertes dar.

- Für das **Accounting** betragen alle Werte in dieser Zeitspanne 0.

Uhrzeit zurückstellen (Sommer- auf Winterzeit)

- In den zeitbasierten Reports gibt es für die entsprechende Zeitspanne schon Log-Daten, die aus Sicht des Systems aber aus der Zukunft kommen: Diese Daten werden nicht überschrieben.
- Die Log-Dateien werden weitergeschrieben, wenn der Zeitpunkt vor dem Zurückstellen wieder erreicht ist.
- Die meisten Diagramme stellen die Werte dieser Zeitspanne zusammengepresst dar.
- Für das **Accounting** behalten die bereits erfassten Daten (aus der Zukunft) ihre Gültigkeit. Die Accounting-Dateien werden weitergeschrieben, wenn der Rückstell-Zeitpunk wieder erreicht ist.

Es wird daher geraten, die Zeit nur bei der Erst-Konfiguration einmalig zu setzen und später nur geringfügig anzupassen. Verwenden Sie am Besten die Central European Time (CET). Dies ist die ursprüngliche Uhrzeit. Das System läuft dann immer in CET, nicht in CEST (Central European Summer Time). Umstellungen von Winter- und Sommerzeit sollten nicht vorgenommen werden, insbesondere wenn die gesammelten Reporting- und Accounting-Daten weiterverarbeitet werden.

Systemzeit manuell einstellen:

1. Öffnen Sie im Verzeichnis **System** das Menü **Settings**.

2. Führen Sie im Fenster **Time Settings** folgende Einstellungen in der angegebenen Reihenfolge durch:

   Use NTP Server: Vergewissern Sie sich für die manuelle Zeiteinstellung, dass hier kein NTP-Server ausgewählt ist. In diesem Fall wird im Drop-down-Menü **Please select** angezeigt.
   Sollte ein NTP-Server eingestellt sein, wählen Sie im Drop-down-Menü **No NTP Server** aus.

   Time Zone: Wählen Sie nun die Zeitzone aus.

Hinweis:

Die neu definierte Zeitzone hat nur eine Auswirkung auf die derzeit eingestellte Uhrzeit, wenn Sie bereits einen NTP-Server eingerichtet haben.

Set Time: Stellen Sie das Datum und die Uhrzeit ein.

Wichtiger Hinweis:

Beachten Sie bei der Eingabe des aktuellen Datums das Ausgabedatum des License Key. Falls das Ausgabedatum des Keys nach dem aktuellen Datum liegt, wird die Lizenz deaktiviert. Es wird nicht automatisch die Evaluation License (30-Tage-Testlizenz) aktiviert.

3. Speichern Sie Ihre Einstellungen durch einen Klick auf die Schaltfläche **Save**.

Die Uhrzeit des Systems wird nun aktualisiert.

Systemzeit mit NTP-Server synchronisieren:

Bevor die Uhrzeit des Internet-Sicherheitssystems mit einem externen System synchronisiert werden kann, muss dieses als **NTP-Server** definiert werden. Der **NTP-Server** wird dabei als Netzwerk bestehend aus einem Rechner definiert.

Das Definieren von Netzwerken wird ausführlich in Kapitel 5.2 ab Seite 134 beschrieben. Wenn der NTP-Server bereits definiert ist, beginnen Sie mit Schritt 6.

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Networks**.
2. Vergeben Sie im Eingabefeld **Name** einen eindeutigen **Namen**. Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9, Minus- und Leerzeichen sowie Unterstrich. Maximal 39 Zeichen sind möglich.
3. Tragen Sie nun die **IP-Adresse** des **NTP-Servers** ein.

4. Im Eingabefeld **Subnet Mask** geben Sie die **Netzwerkmaske** 255.255.255.255 ein.

5. Bestätigen Sie nun Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

   WebAdmin prüft nun Ihre Eingaben auf semantische Gültigkeit. Nach erfolgreicher Definition wird das neue Netzwerk in die Netzwerk-Tabelle eingetragen.

6. Öffnen Sie im Verzeichnis **System** das Menü **Settings**.

7. Führen Sie im Fenster **Time Settings** folgende Einstellungen in der angegebenen Reihenfolge durch:

   Time Zone: Wählen Sie zuerst die Zeitzone aus.

   Use NTP Server: Wählen Sie hier den NTP-Server aus.

Die Uhrzeit des Internet-Sicherheitssystems wird nun mit dem externen System jede volle Stunde synchronisiert.

SSH (Shell Access) Settings



Die **Secure Shell (SSH)** ist eine textorientierte Schnittstelle zum Internet-Sicherheitssystem, die nur für erfahrene Administratoren geeignet ist. Man benötigt für den Zugriff per **SSH** einen **SSH-Client**, der in den meisten Linux-Distributionen bereits vorhanden ist. Unter MS Windows ist das Programm **Putty** als **SSH-Client** zu empfehlen. Der Zugriff per **SSH** ist verschlüsselt und somit für Fremde nicht mitzulesen.

Die Funktion Shell Access ist per Default eingeschaltet, wenn Sie im Fenster **Setting System Passwords** für die Konfiguration über den **Astaro Configuration Manager** ein Passwort gesetzt haben.

Wenn Sie über **SSH** auf das Internet-Sicherheitssystem zugreifen wollen, muss der SSH-Status eingeschaltet sein (Statusampel zeigt Grün). **SSH** benötigt für die Protokollierung des Zugriffs **Namensauflösung** (gültige Nameserver), anderenfalls gibt es bei der SSH-Anmeldung einen Time-out. Dieser Time-out dauert etwa eine Minute an. In dieser Zeit sieht es so aus, als wäre die Verbindung eingefroren oder würde nicht zustande kommen. Danach geht es ohne Verzögerung weiter.

Zusätzlich müssen Sie im Auswahlfeld **Allowed Networks** die Netzwerke hinzufügen, von denen aus per **SSH** auf das Internet-Sicherheitssystem zugegriffen werden soll.
Per Default-Einstellung ist im Auswahlfeld **Allowed Networks** für eine reibungslose Installation die Option **Any** eingetragen, d. h. jeder ist berechtigt auf den SSH-Dienst zuzugreifen. Netzwerke definieren Sie im Menü **Definitions/Networks**.

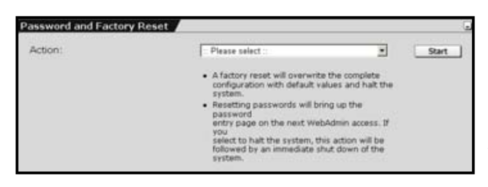


Sicherheitshinweis:

Per Default-Einstellung ist jeder berechtigt auf den SSH-Dienst zuzugreifen. Im Auswahlfeld **Allowed Networks** ist die Option **Any** eingetragen. Aus Sicherheitsgründen empfehlen wir den Zugriff auf den SSH-Dienst zu beschränken. Alle anderen Netzwerke sollten sie löschen!

Schalten Sie aus Sicherheitsgründen den **SSH**-Zugang nach Abschluss der Arbeiten wieder ab.

Password and Factory Reset



Mit **Password Reset** können Sie die Passwörter für das Internet-Sicherheitssystem neu setzen. Wenn Sie sich nach dieser Aktion das nächste mal im Konfigurationstool **WebAdmin** anmelden, wird das Fenster **Setting System Passwords** angezeigt. Auf diese Weise können Sie optionale Passwörter, wie z. B. das Astaro-Configuration-Manager-Passwort nachträglich setzen. Mit **Halt System** wird das Internet-Sicherheitssystem zusätzlich heruntergefahren. Nach dem Neustart wird dann zuerst das Fenster **Setting System Passwords** angezeigt.

Mit **Factory Reset** wird das Sicherheitssystem in den ursprünglichen Zustand nach der Installation zurückgesetzt, d. h. alle Daten, die nach der Installation auf dem System erzeugt oder eingegeben wurden, werden gelöscht. Dies betrifft insbesondere die gesamte Konfiguration, den **HTTP Proxy Cache**, die **E-Mail Queues**, die **Accounting**- und **Reporting**-Daten, alle Passwörter und alle noch nicht installierten **Up2Dates**.
Der Versionsstand des Internet-Sicherheitssystems bleibt erhalten, alle installierten **System Up2Dates** und **Pattern Up2Dates** werden nicht verändert.

Hinweis:

Bei einem **High-Availability (HA)**-System muss der **Factory Reset** bei beiden Sicherheitssystemen (Normal- und Hot-Standby-Modus) separat durchgeführt werden.

Zusammensetzung der Passwörter:

Um die Sicherheit für das Sicherheitssystem und somit auch für das interne Netzwerk zu erhöhen unterliegt die Zusammensetzung und die Länge des Passworts den nachfolgend aufgeführten Restriktionen. Das Passwort wird vom Sicherheitssystem nur übernommen, wenn diese Bestimmungen erfüllt sind:

- eine Mindestlänge von acht Zeichen
- mindestens ein kleingeschriebener Buchstabe
- mindestens ein großgeschriebener Buchstabe
- mindestens eine Zahl
- mindestens ein nicht-alphanumerisches Zeichen (innerhalb der ASII-Tabelle, Zeile 32 bis 126)

Die Restriktionen für die Passwörter sind nur für neu Installierte Sicherheitssysteme ab Version 6.105 gültig oder treten in Kraft falls ab der Version 6.105 die Aktion **Passwort Reset** oder **Factory Reset** durchgeführt wurde.

5.1.2. Licensing



Die Lizenzierung des Internet-Sicherheitssystems erfolgt im Registrierungsportal von **MyAstaro** (die Adresse lautet http://my.astaro.com). Über *MyAstaro* können Sie eine 30-Tage-Testversion herunterladen und diese später in eine Unternehmensversion umwandeln.

Der Preis für die Unternehmensversion richtet sich nach der Größe des zu schützenden Netzwerks, des Support-Umfangs und der zusätzlich zur Basislizenz abonnierten Funktions- und Sicherheitspakete.

Die Basislizenz und die drei Funktions- und Sicherheitspakete enthalten die folgenden Module:

- Basislizenz: Firewall, VPN Gateway und Intrusion Protection
- Maintenance: Up2Date Service und Technical Support
- Secure E-Mail Subscription: Spam Protection, Virus Protection for E-Mail
- Secure Web Subscription: Surf Protection (URL Filtering), Virus Protection for Web

Zur Lizenzierung einer Unternehmensversion benötigen Sie zuerst den **Activation Key**. Mit diesem *Activation Key* aktivieren Sie anschließend im Registrierungsportal von **MyAstaro** den **License Key**. Nur dieser *License Key* kann im Sicherheitssystem eingespielt werden! Auf diese Weise können Sie selbst den Beginn des Lizenzzeitraums Ihres Sicherheitssystems bestimmen: Sie installieren zuerst die Software und registrieren anschließend Ihre Lizenz – erst in diesem Augenblick beginnt die Zeitspanne für die abonnierte Unternehmensversion und die erworbenen Module.

Weitere Informationen zur Lizenzierung sowie den entsprechenden **Activation Key** erhalten Sie bei einem zertifizierten *Astaro*-Partner oder Sie wenden sich über die E-Mail-Adresse **sales@astaro.com** direkt an *Astaro*.

Hinweis:

Der **Activation Key** kann nicht direkt über das Konfigurationstool **WebAdmin** auf dem Sicherheitssystem eingespielt werden. Der *Activation Key* dient nur zur Aktivierung des **License Key**. Nur dieser *License Key* kann auf dem Sicherheitssystem eingespielt werden.

Benutzer-Account festlegen:

1. Öffnen Sie mit Ihrem Browser die Internetseite mit der Adresse https://my.astaro.com.

2. Melden Sie sich in **MyAstaro** an.

   What is your e-mail address?

   Für die Authentifizierung wird die E-Mail-Adresse verwendet. Als Neukunde tragen Sie hier Ihre E-Mail-Adresse ein.

   Wenn Sie bereits das **Registration Portal** genutzt haben, tragen Sie in das Eingabefeld die E-Mail-Adresse ein, die Sie bei der Anmeldung verwendet haben. Falls Sie die damals verwendete E-Mail-Adresse nicht mehr wissen, können Sie diese unter dem Dialog **Returning Registration Portal users** abfragen. Sie benötigen Ihr **Username** und das **Password**.

   Do you have a MyAstaro password?

   Falls Sie sich zum ersten Mal in *MyAstaro* anmelden, klicken Sie das Auswahlkästchen bei **No, I am a new user** an. Falls Sie bereits Benutzer von MyAstaro sind, tragen Sie das Passwort in das Eingabefeld **Yes, my password is** ein.

   Klicken Sie anschließend auf die Schaltfläche **Submit**.

3. Generieren Sie einen **MyAstaro Accout**.

E-Mail Address: In diesem Eingabefeld können Sie Ihre Adresse korrigieren.

Password: Tragen Sie Ihr gewünschtes Passwort ein.

First Name: Tragen Sie Ihren Vornamen ein.

Last Name: Tragen Sie Ihren Nachnamen ein.

Klicken Sie anschließend auf die Schaltfläche **Register**.

Bei erfolgreicher Registrierung wird nun die Seite mit der Meldung **Congratulations, you have created your MyAstaro account**. Des Weiteren wird Ihnen per E-Mail eine Bestätigung zugesendet.

Sie können nun in **MyAstaro** verschiedene Versionen des Internet-Sicherheitssystems herunterladen und zu Ihrer Lizenz die folgenden Aktionen durchführen:

1. Version 5-Lizenzen zu Version 6-Lizenzen konvertieren
2. gekaufte Version-6-Activation-Keys registrieren
3. Optionen zu registrierten Lizenzen hinzufügen
4. eine kostenlose Home-User-Lizenz herunterladen
5. eine funktionserweiterte 30-Tage-Testversion herunterladen

Internet-Sicherheitssystem lizenzieren:

Für die Lizenzierung des Internet-Sicherheitssystems benötigen Sie die gültige Lizenzdatei (*License Key*) auf dem lokalen Host, damit Sie diese über das Konfigurationstool **WebAdmin** in das Sicherheitssystem importieren können.

Hinweis:

Bei einer Lizenz mit der Option **High Availability (HA)** müssen Sie den **License Key** auf beiden Sicherheitssystemen (Normal- und Hot-Standby-Modus) einspielen.

---

1. Öffnen Sie im Verzeichnis **System** das Menü **Licensing**.
2. Klicken Sie beim Eingabefeld **Upload License File** auf die Schaltfläche **Durchsuchen**.
3. Wählen Sie über den Dialog **Datei auswählen** die Lizenzdatei aus und klicken anschließend auf die Schaltfläche **Öffnen**.
4. Klicken Sie auf die Schaltfläche **Start**.

Die Installation der Lizenzdatei dauert ca. 30 bis 60 Sekunden. Nach erfolgreicher Registrierung des Internet-Sicherheitssystems erhalten Sie im Fenster **License Information** Angaben zu Ihrer Lizenz.

Licensing Information

Nach erfolgreicher Registrierung des Internet-Sicherheitssystems werden in in diesem Fenster die Lizenz-Informationen angezeigt.

Licensed Users (IPs)

Die Funktionen in diesem Fenster sind für Lizenzen, die keine unbegrenzte Anzahl an Benutzern (IP-Adressen) zulassen.

Current User (IP) Listing: In der Tabelle sind alle IP-Adressen aufgelistet, die für die Lizensierung relevant sind. The aktuelle Benutzertabelle wird immer geladen wenn dieses Menü geöffnet wird.
Die Tabelle wird auch angezeigt, wenn es sich bei der Lizenz um eine Unlimited-Version handelt.

Reset User (IPs) Listing: Wenn Sie das interne Netzwerk neu konfigurieren möchten, können Sie durch diese Aktion die Tabelle mit den Benutzern zurücksetzen. Anschließend erfolgt ein Reboot - das Internet-Sicherheitssystem wird heruntergefahren und wieder gestartet.
Die Aktion wird durch einen Klick auf die Schaltfläche **Start** eingeleitet.

5.1.3. Up2Date Service



Mit dem **Up2Date Service** halten Sie Ihr System auf dem neusten Stand: Neue Viren-Pattern, System-Patches und Sicherheits-Features werden in Ihr laufendes System eingespielt.

Die **Up2Date**-Pakete sind signiert - nur Astaro ist berechtigt, solche **Up2Date**-Pakete zu erstellen und zu signieren. Nicht korrekt signierte **Up2Date**-Pakete werden als solche erkannt und gelöscht. Für **System Up2Date** und für **Pattern Up2Date** gibt es mehrere Up2Date-Server, die der Reihe nach angewählt werden. Falls ein Up2Date-Server nicht erreichbar ist, wird der nächste Server nach System- bzw. Pattern Up2Dates abgefragt.

Wichtiger Hinweis:

Der **Up2Date Service** benutzt eine TCP-Verbindung auf Zielport 443, um die Up2Date-Pakete herunterzuladen. Das Internet-Sicherheitssystem selbst erlaubt diese Verbindung ohne weitere Einstellungen. Falls Sie jedoch eine übergeordnete (*Upstream*) Firewall verwenden, müssen Sie auf dieser die Kommunikation über Port 443 TCP zu den Update-Servern erlauben. Des Weiteren muss auf dem *Upstream-Proxy* das **Virus Protection** für die Up2Date-Verbindung ausgeschaltet werden. Definieren Sie hierfür ein **Profile** in der **Surf-Protection-Profile**-Tabelle und lassen die Funktion **Virus Protection for Web** ausgeschaltet.

Weitere Informationen zur Konfiguration des **Surf Protection Profile** erhalten Sie in Kapitel 5.6.1.1 ab Seite 279.

Wichtiger Hinweis:

Bei Sicherheitssystemen *hinter* einem *Upstream-Proxy* muss für das Herunterladen der Up2Date-Pakete immer der **DNS-Proxy** eingeschaltet werden. Die dafür notwendige Namensauflösung erfolgt nicht automatisch über den Upstream-Proxy.
Die Konfiguration des **DNS-Proxy** wird in Kapitel 5.6.4 ab Seite 336 beschrieben.

System Up2Date

Mit dem Modul **System Up2Date** importieren Sie System-Patches und neue Sicherheits-Features auf Ihr Internet-Sicherheitssystem. Die **Up2Date**-Pakete können manuell oder automatisch vom Update-Server heruntergeladen werden. Falls Sie nicht über eine Internetverbindung verfügen, können die Up2Date-Pakete von einem lokalen Datenträger aus eingespielt werden.

Neu eingespielte Up2Date-Pakete werden in der Tabelle **Unapplied Up2Dates** mit der Versionsnummer und dem Dateinamen angezeigt. Diese Up2Date-Pakete sind noch nicht installiert!
Weitere Informationen erhalten Sie, wenn Sie mit dem Cursor die **blaue Info-Schaltfläche** berühren. Falls die Info-Schaltfläche in **rot** angezeigt wird, wird nach der Installation des *System-Up2Date*-Pakets automatisch ein **Restart** des Sicherheitssystems durchgeführt.

Hinweis:

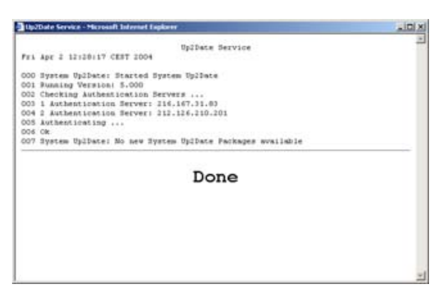
Beachten Sie beim **High Availability (HA)**-System die zusätzlichen Hinweise zum Einspielen und Installieren der **System Up2Dates**. Das **HA**-System wird in Kapitel 5.1.11 ab Seite 122 erklärt.

Fehlende Up2Date-Pakete können Sie unter der Internetadresse **http://download.astaro.de/ASL/up2date** auf Ihren lokalen Rechner herunterladen.

System Up2Date manuell einspielen:

1. Öffnen Sie im Verzeichnis **System** das Menü **Up2Date Service**.

2. Klicken Sie im Fenster **System Up2Date** auf die Schaltfläche **Start** bei **Prefetch Up2Dates now**.



Das System prüft nun, ob auf dem Update-Server neue Up-2Date-Pakete vorhanden sind und lädt diese herunter. Der gesamte Up2Date-Vorgang wird im **Log-Fenster** in Echtzeit dargestellt (linkes Bild). Der Vorgang wurde erfolgreich beendet, wenn im Fenster die Meldung **DONE** erscheint.

Die in der Tabelle **Unapplied Up2Dates** aufgelisteten Up2Date-Pakete sind noch nicht installiert!

Beim **HA**-System werden die neuen Up2Date-Pakete in der Tabelle **Unapplied Up2Dates Master** angezeigt.

System Up2Date über Internet automatisch einspielen:

1. Öffnen Sie im Verzeichnis **System** das Menü **Up2Date Service**.

2. Schalten Sie die Funktion durch einen Klick auf die Schaltfläche **Enable** bei **Prefetch Up2Dates automatically** ein.

3. Definieren Sie im Auswahlfeld **Interval** den Zeitabstand, nach dem das System automatisch den spezifizierten Update-Server anwählt und diesen auf neue **System Up2Dates** überprüft.

   Die möglichen Zeitintervalle sind: Jede Stunde (every hour), jeden Tag (every day), einmal pro Woche (every week).

Neu eingespielte Up2Date-Pakete werden in der Tabelle **Unapplied Up2Dates** mit der Versionsnummer und dem Dateinamen angezeigt. Weitere Informationen erhalten Sie mit Hilfe der Info-Schaltfläche.
Die in der Tabelle aufgelisteten Up2Date-Pakete sind noch nicht installiert!

Beim **HA**-System werden die neuen Up2Date-Pakete in der Tabelle **Unapplied Up2Dates Master** angezeigt.

System Up2Date von lokalem Datenträger einspielen:

Der Dateiname eines Up2Date-Pakets setzt sich aus der Versionsnummer, der Bezeichnung **tar** für ein verschlüsseltes Archiv und dem Dateitype **.gpg** zusammen. Beispiel: 5.009.tar.gpg. Up2Date-Pakete finden Sie auf dem FTP-Server **ftp.astaro.com**.

1. Öffnen Sie im Verzeichnis **System** das Menü **Up2Date Service**.
2. Klicken Sie im Fenster **System Up2Date** auf die Schaltfläche **Durchsuchen** bei **Import from File**.
3. Wählen Sie im Fenster **Datei auswählen** das Up2Date-Paket aus, das Sie importieren möchten und klicken auf die Schaltfläche **Öffnen**.

Wichtiger Hinweis:

Verwenden Sie zum Importieren der Up2Date-Pakete unter Microsoft Windows keinen **UNC-Pfad**. Wählen Sie die Pakete mit Hilfe des Auswahlfeldes **Durchsuchen** aus.

4. Klicken Sie im Fenster **System Up2Date** bei **Import from File** auf die Schaltfläche **Start**.

   Neu eingespielte Up2Date-Pakete werden anschließend in der Tabelle **Unapplied Up2Dates** mit der Versionsnummer und dem Dateinamen angezeigt. Weitere Informationen erhalten Sie mit Hilfe der Info-Schaltfläche.

Die in der Tabelle aufgelisteten Up2Date-Pakete sind noch nicht installiert!

Beim **HA**-System werden die neuen Up2Date-Pakete in der Tabelle **Unapplied Up2Dates Master** angezeigt.

5. Wiederholen Sie nun die Schritte 2 bis 4 bis Sie alle Up2Date-Pakete importiert haben.

System Up2Date installieren (ohne HA-System):

1. Öffnen Sie im Verzeichnis **System** das Menü **Up2Date Service**.
2. Wählen Sie in der Tabelle **Unapplied Up2Dates** das Up2Date-Paket aus.

Hinweis:

Falls die Tabelle mehr als ein **System Up2Date**-Paket enthält, starten Sie die Installation mit der **aktuellsten** Version. Die älteren Versionen werden dann automatisch installiert.

3. Klicken Sie nun in der Spalte **Actions** auf **Install**.

Die Installation der Up2Date-Pakete wird im **Log-Fenster** in Echtzeit dargestellt. Der Vorgang wurde erfolgreich beendet, wenn im Fenster die Meldung **DONE** erscheint.

System Up2Date auf HA-Lösung installieren:

1. Öffnen Sie im Verzeichnis **System** das Menü **Up2Date Service**.
2. Wählen Sie in der Tabelle **Unapplied Up2Dates Master** das Up2Date-Paket aus.

Hinweis:

Falls die Tabelle mehr als ein **System Up2Date**-Paket enthält, starten Sie die Installation mit der **kleinsten** Version. Auf dem **HA**-System kann immer nur ein Paket installiert werden.

3. Klicken Sie nun in der Spalte **Actions** auf **Install**.

   Die Installation des Up2Date-Pakets auf dem System 1 wird im **Log-Fenster** in Echtzeit dargestellt. Der Vorgang wurde erfolgreich beendet, wenn im Fenster die Meldung **DONE** erscheint.

   Anschließend wird die Installation automatisch auf dem System 2 gestartet. In der Tabelle **Unapplied Up2Dates Slave** wird während des Vorgangs das Up2Date-Paket und die Meldung **Polled by slave** angezeigt.
   Die Installation auf dem System 2 wurde erfolgreich beendet, wenn in der Tabelle wieder die Meldung **No locally stored Up2Date packages available** erscheint.

4. Falls in der Tabelle **Unapplied Up2Dates Master** noch Up2-Date-Pakete angezeigt werden, wiederholen Sie die Schritte 2 und 3 solange bis keine Up2Date-Pakete mehr verfügbar sind.

   Auf dem **HA**-System wurden alle verfügbaren Up2Date-Pakete installiert, wenn in der Tabelle **Unapplied Up2Dates Master** die Meldung **No locally stored Up2Date packages available** erscheint und die angezeigten Versionen der beiden Systeme übereinstimmen.

Pattern Up2Date



Durch die Funktion **Pattern Up2date** werden die *Anti-Virus Engines*, das *Spam Protection* und das *Intrusion Protection System (IPS)* mit neuen Patterns, bzw. IPS-Angriffssignaturen aktualisiert. Sie haben die Möglichkeit, die Sicherheits-Abonnements manuell oder automatisch in bestimmten Zeitintervallen auf dem neusten Stand zu halten.

Die Tabelle **Latest Pattern Up2Dates** informiert Sie, welche **Pattern-Up2Date**-Pakete zuletzt installiert wurden: Die Virus Protection Patterns für die *Astaro AV Engine* und für die *Open Source Engine*, die Spam Protection Patterns und die Intrusion-Protection-Angriffssignaturen werden separat aufgelistet. Es werden nur die Pattern Up2Dates für die installierten Security Subscriptions angezeigt.
Die Sicherheits-Abonnements (Subscriptions) werden in Kapitel 5.1.2 auf Seite 56 beschrieben.

Pattern Up2Date, manuell:

1. Öffnen Sie im Verzeichnis **System** das Menü **Up2Date Service**.
2. Klicken Sie im Fenster **Pattern Up2Date** auf die Schaltfläche **Start** bei **Update now**.

Das System prüft nun, ob auf dem Update-Server neue Pattern Up2Date-Pakete vorhanden sind, lädt diese herunter und installiert sie auf dem Internet-Sicherheitssystem. Der gesamte Up2Date-Vorgang wird im **Log-Fenster** in Echtzeit dargestellt. Der Vorgang wurde erfolgreich beendet, wenn im Fenster die Meldung **DONE** erscheint.

Die **Datumsangabe** (**Date**) wird aktualisiert, wenn Sie im Verzeichnis **System** auf **Up2Date Service** klicken oder sobald Sie das nächste Mal dieses Menü öffnen.

Bei der **High Availability (HA)**-Lösung wird der Virusscanner von System 2 automatisch mit dem von System 1 synchronisiert.

Pattern Up2Date, automatisch:

1. Öffnen Sie im Verzeichnis **System** das Menü **Up2Date Service**.
2. Schalten Sie die Funktion durch einen Klick auf die Schaltfläche **Enable** bei **Update automatically** ein.
3. Definieren Sie im Auswahlfeld **Interval** den Zeitabstand, nach dem das Internet-Sicherheitssystem automatisch den spezifizierten **Up2Date Server** anwählt und diesen auf neue **Pattern Up2Dates** überprüft.

   Die möglichen Zeitintervalle sind: Jede Stunde (Hourly), jeden Tag (Daily), einmal pro Woche (Weekly).



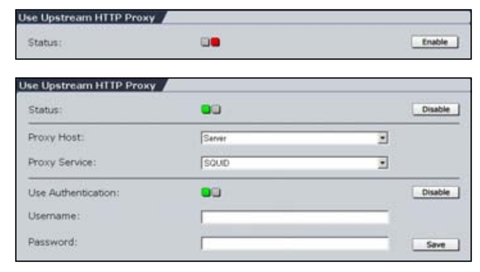
Sicherheitshinweis:

Stellen Sie das Intervall auf jede Stunde ein, damit Ihr Virenscanner immer auf dem aktuellsten Stand ist.

Der automatische **Pattern Up2Date** ist jetzt aktiviert. Das Internet-Sicherheitssystem prüft nun regelmäßig auf dem **Up2Date Server** ob neue **Pattern Up2Dates** zur Verfügung stehen. Sobald ein neues **Pattern Up2Date** installiert ist, erhält der Administrator eine E-Mail, in der die zuletzt installierten Virensignaturen aufgelistet sind.

Beim **High-Availability-(HA)**-System wird der Virusscanner von System 2 automatisch mit dem von System 1 synchronisiert.

Use Upstream HTTP Proxy



In diesem Fenster können Sie die Verbindung zu einem **Upstream Proxy Server** definieren. Diese Funktion benötigen Sie, falls Sie nur über einen solchen Upstream Proxy HTTP- und HTTPS-Ports erreichen können.

Upstream Proxy Server definieren:

1. Öffnen Sie im Verzeichnis **System** das Menü **Up2Date Service**.

2. Schalten Sie im Fenster **Use Upstream HTTP Proxy** den Proxy durch einen Klick auf die Schaltfläche **Enable** ein.

   Anschließend öffnet sich ein erweitertes Eingabefenster.

3. Definieren Sie in den **Upstream HTTP Proxy**.

   Proxy Host: Wählen Sie im Drop-down-Menü den Proxy-Server aus. Der Server muss zuvor im Menü **Definitions/Networks** definiert werden.

   Proxy Service: Wählen Sie im Drop-down-Menü den Dienst aus. Der Dienst muss zuvor im Menü **Definitions/Services** definiert werden.

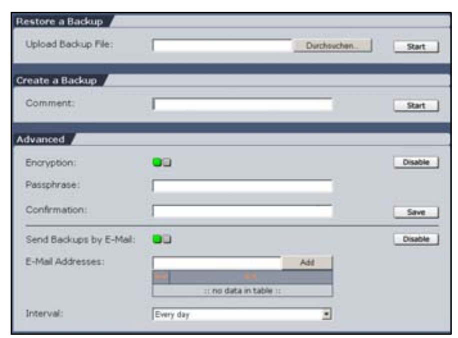
4. Falls für den **Upstream Proxy Server** eine Authentifizierung notwendig ist, klicken Sie auf die Schaltfläche **Enable**.

   Username: Tragen Sie in das Eingabefeld den Benutzernamen ein.

   Password: Tragen Sie in das Eingabefeld das Passwort ein.

5. Speichern Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

5.1.4. Backup



Mit der Funktion **Backup** können Sie die Einstellungen Ihres Internet-Sicherheitssystems auf einer lokalen Festplatte sichern. Mit Hilfe der Backup-Datei sind Sie in der Lage, ein neu installiertes System auf einen identischen Konfigurationsstand zu bringen. Dies ist bei einem Hardware-Defekt besonders hilfreich, da binnen Minuten ein neues Sicherheitssystem installiert und anschließend das Backup eingespielt werden kann. Bereits nach kurzer Zeit ist auf diese Weise ein Ersatzsystem einsatzbereit.

Achtung:

In die aktuelle Software-Version 6 kann nur ein Backup aus der Version 5.200 oder höher eingespielt werden.

Tragen Sie im Menü **Licensing** zuerst den License Key ein und spielen anschließend das Backup ein. Vom System werden sonst nur drei Netzwerkkarten hochgefahren und dies kann dazu führen, dass das Konfigurationstool **WebAdmin** nicht mehr erreichbar ist.

Hinweis:

Legen Sie nach jeder Änderung der Systemeinstellungen eine neue Backup-Datei an. Auf diese Weise haben Sie immer die aktuellen Einstellungen Ihres Systems gespeichert. Bewahren Sie dieses Backup an einem sicheren Ort auf, da alle Konfigurations-Einstellungen, z. B. die Zertifikate und Keys, darin enthalten sind.

Prüfen Sie die Backup-Datei nach der Generierung immer auf Lesbarkeit. Es ist außerdem ratsam durch ein externes MD5-Programm eine Prüfsumme zu generieren, die es Ihnen auch später ermöglicht, die Funktionsfähigkeit der Backup-Datei zu prüfen.

Restore a Backup

Die Backup-Datei kann im Bedarfsfall auf zwei Arten auf dem Sicherheitssystem installiert werden: manuell über das Fenster **Restore a Backup** oder ab der Software-Version 6.203 automatisch während des Systemneustarts über einen an das Sicherheitssystem angeschlossenen **USB-Speicher-Stick**.

Während eines Neustarts wird vom System geprüft ob an einer USB-Schnittstelle (Universal Serial Bus) ein entsprechendes Speichermedium angeschlossen ist und ob sich darauf Dateien mit der Erweiterung **abf** (astaro backup file) befinden. Falls eine Backup-Datei vorhanden ist, wird diese automatisch auf dem Sicherheitssystem installiert. Anschließend wird das Sicherheitssystem neu gestartet.

Falls der USB-Speicher als Lese- und Schreibmedium genutzt werden kann, werden auf diesem zur Auswertung des Wiederherstellungsprozesses relevante Informationen gespeichert.

Solange der USB-Speicher an das Sicherheitssystem angeschlossen bleibt, verhindert eine vom System generierte Lock-Datei, dass die Backup-Datei nicht immer wieder neu installiert wird. Falls Sie beabsichtigen die bereits eingespielte Backup-Datei neu zu installieren,

muss zuvor die Lock-Datei gelöscht werden. Dies erfolgt, indem Sie das Sicherheitssystem ohne den USB-Speicher neu starten.

Wichtiger Hinweis:

Eine mit der Funktion **Encryption** verschlüsselte Backup-Datei kann nicht über den **USB Stick** installiert werden. Die Funktion *Encryption* wird auf Seite 74 beschrieben.

Im nachfolgenden Abschnitt wird beschrieben wie die Backup-Datei manuell über das Fenster **Restore a Backup** installiert wird.

Backup manuell installieren:

1. Öffnen Sie im Verzeichnis **System** das Menü **Backup**.
2. Klicken Sie im Fenster **Restore a Backup**, neben dem Eingabefeld **Upload Backup File** auf die Schaltfläche **Durchsuchen**.
3. Wählen Sie im Fenster **Datei auswählen** die Backup-Datei aus, die Sie importieren möchten und klicken auf die Schaltfläche **Öffnen**.

   Hinweis:

   Verwenden Sie zum Einspielen des Backups unter Microsoft Windows keinen **UNC-Pfad**. Wählen Sie die Backup-Datei mit Hilfe des Auswahlmenüs **Suchen in** aus.

4. Bestätigen Sie die Eingabe durch einen Klick auf die Schaltfläche **Start**.

   Die Sicherungsdatei wird anschließend auf das System geladen und überprüft. Wenn die Prüfsummen stimmen, erhalten Sie nun die **Backup Information**.

5. Überprüfen Sie die **Backup Information**.
6. Übernehmen Sie die Backup-Datei in das aktive System durch einen Klick auf die Schaltfläche **Start**.

Wenn die Meldung **Backup has been restored successfully** erscheint, wurde der Vorgang erfolgreich abgeschlossen.

Create a Backup

In diesem Fenster können Sie von der Konfiguration auf dem Sicherheitssystem eine Backup-Datei erstellen und archivieren.

Backup manuell generieren:

1. Öffnen Sie im Verzeichnis **System** das Menü **Backup**.
2. Geben Sie im Fenster **Create a Backup** in das Eingabefeld **Comment** einen Kommentar ein.
   Wenn Sie später das Backup wieder einspielen, erscheint der Kommentar in der Information.

   Wichtiger Hinweis:

   Falls die Funktion **Encryption** eingeschaltet ist, wird die Backup-Datei mit **DES** oder **3DES** verschlüsselt und kann später nur mit dem richtigen Passwort wieder eingespielt werden.

   ---

3. Um die Backup-Datei zu erzeugen, klicken Sie auf die Schaltfläche **Start**.

   Das System generiert nun die Backup-Datei. Wenn die Meldung **Backup has been created successfully** erscheint, wurde der Vorgang erfolgreich abgeschlossen.
4. Um die Backup-Datei auf Ihren lokalen PC zu speichern, klicken Sie nun auf die Schaltfläche **Save**.
5. Wählen Sie in dem Menü **Dateidownload** die Option **Datei auf Datenträger speichern** aus und klicken Sie auf die Schaltfläche **OK**.

6. Im Menü **Datei speichern unter** können Sie die Datei nun unter einem beliebigen Dateinamen speichern.
   Der vom Sicherheitssystem erzeugte Dateinamen setzt sich aus Backup, Datum und Uhrzeit zusammen:
   backup_yyyymmdd_hhmmss.abf (astaro-backup-file).

7. Prüfen Sie die neu generierte Datei auf Lesbarkeit, indem Sie die Backup-Datei importieren und auf die Schaltfläche **Start** klicken.

   Die Sicherungsdatei wird anschließend auf das System geladen und überprüft. Wenn die Prüfsummen stimmen, erhalten Sie nun die **Backup Information**.

8. Brechen Sie anschließend den Einspielvorgang ab, indem Sie auf ein Menü im Verzeichnis klicken.

Achtung:

Generieren Sie nach jeder Änderung im System eine neue Backup-Datei. Wenn Sie eine Backup-Datei einspielen und etwa zwischenzeitlich das Passwort oder die IP-Adresse des Sicherheitssystems geändert haben, kann es passieren dass Sie keinen Zutritt mehr zum System erhalten.

Advanced

Encryption: Die Backup-Datei enthält alle Konfigurations-Einstellungen sowie die darin enthaltenen Zertifikate und Keys. Mit der Funktion **Encryption** kann die Datei mit **DES** oder **3DES** verschlüsselt werden.

Wichtiger Hinweis:

Die Backup-Datei kann ab der Software-Version 6.203 auch automatisch über einen an das Sicherheitssystem angeschlossenen **USB-Speicher-Stick** installiert werden. Mit der Funktion **Encryption** verschlüsselte Backup-Dateien können nicht über den *USB-Speicher* installiert werden!

E-Mail Backup File verschlüsseln:

1. Öffnen Sie im Verzeichnis **System** das Menü **Backup**.
2. Scrollen Sie zum Fenster **Advanced**.
3. Schalten Sie die Funktion **Encryption** durch einen Klick auf die Schaltfläche **Enable** ein.

   Die Funktion **Encryption** ist eingeschaltet, wenn die Statusampel Grün zeigt.
4. Tragen Sie in das Eingabefeld **Passphrase** das Passwort ein.

   Sicherheitshinweis:

   Bei einem Passwort mit bis zu sieben Zeichen wird die Backup-Datei mit **DES** verschlüsselt, ab acht Zeichen mit **3DES**.
5. Tragen Sie das Passwort zur Bestätigung nochmals in das Eingabefeld **Confirmation** ein.
6. Speichern Sie die Einstellungen durch einen Klick auf die Schaltfläche **Save**.

Alle Backup-Dateien, die nun von Ihnen manuell oder vom System automatisch generiert werden, sind mit dem definierten Passwort verschlüsselt.

Wichtiger Hinweis:

Eine mit **Encryption** verschlüsselte Backup-Datei kann nur wieder auf dem System eingespielt werden, wenn das Passwort der verschlüsselten Datei und das aktuelle Passwort auf dem Sicherheitssystem identisch sind. Falls Sie das Passwort ändern, sollten Sie daher zur Sicherheit eine neue Backup-Datei generieren.

Send Backups by E-Mail: Damit Sie nicht ständig daran denken müssen die Einstellungen Ihres Internet-Sicherheitssystems manuell auf einem Datenträger zu sichern, können Sie hier die Backup-Datei automatisch erzeugen lassen. Im Anschluss wird die Datei an die angegebene E-Mail-Adresse geschickt. Eine E-Mail-Backup-Datei ist ca. 100 KB groß.

E-Mail Backup File generieren:

1. Öffnen Sie im Verzeichnis **System** das Menü **Backup**.
2. Schalten Sie im Fenster **Advanced** die Funktion **Send Backups by E-Mail** durch einen Klick auf die Schaltfläche **Enable** ein.

   Die Funktion **Backups by E-Mails** ist eingeschaltet, wenn die Statusampel Grün zeigt.

   Wichtiger Hinweis:

   Falls die Funktion **Encryption** eingeschaltet ist, wird die Backup-Datei mit **DES** oder **3DES** verschlüsselt und kann später nur mit dem richtigen Passwort wieder eingespielt werden.

   ---

3. Definieren Sie mit dem Drop-down-Menü **Interval** den Zeitabstand nach dem automatisch eine neue Backup-Datei erstellt werden soll.

Die möglichen Zeitintervalle sind: Täglich (daily), einmal pro Woche (weekly) und einmal pro Monat (monthly).

4. Tragen Sie in das Eingabefeld **E-Mail Addresses** die Adresse ein, an die die automatisch erstellten Backup-Dateien in regelmäßigen Abständen gesendet werden soll.

5. Durch einen Klick auf die Schaltfläche **Add** neben dem Eingabefeld **E-Mail to** übernehmen Sie die neue Adresse in das Hierarchiefeld.

   Wenn Sie weitere E-Mail-Adressen hinzufügen möchten, wiederholen Sie den Schritt 5.

6. Falls die erste Backup-Datei sofort generiert und abgeschickt werden soll, klicken Sie auf die Schaltfläche **Start** neben **Send Backup now**.

7. Prüfen Sie die neu generierten Dateien auf Lesbarkeit, indem Sie die jeweilige Backup-Datei importieren und auf die Schaltfläche **Start** klicken.

   Die Sicherungsdatei wird anschließend auf das System geladen und überprüft. Wenn die Prüfsummen stimmen, erhalten Sie nun die **Backup Information**.

8. Brechen Sie anschließend den Einspielvorgang ab, indem Sie auf ein Menü im Verzeichnis klicken.

E-Mail-Adressen bearbeiten:

Die Funktionsweise des **Hierarchiefeldes** wird in Kapitel 4.3.5 ab Seite 43 beschrieben.

5.1.5. Anti-Virus (AV) Engines



Für die Sicherheits-Abonnements Virus Protection for E-mail und Virus Protection for Web stehen zwei voneinander unabhängige Anti-Virus Engines zur Verfügung: Die **Astaro AV Engine** und die **Open Source AV Engine**.

Das Sicherheitssystem unterstützt zusätzlich einen Hardware Accelerator mit einem eigenständigen Virenscanner.

Die Anti-Virus (AV) Engines können für die Proxies HTTP, SMTP, POP3 aktiviert werden. Die AV Engines werden automatisch eingeschaltet, nachdem die entsprechenden Sicherheits-Abonnements **E-mail Security** und **Web Security** auf dem Sicherheitssystem installiert sind. Die Sicherheits-Abonnements (Subscriptions) werden in Kapitel 5.1.2 auf Seite 56 beschrieben.

Tipp:

Die beiden *Software Anti-Virus Engines* nutzen für den Scann-Prozess unterschiedliche Verfahren. Wenn Sie bei den Proxies immer beide *Software Anti-Virus Engines* einzuschalten wird daher eine hohe Sicherheitsstufe erreicht.

Hardware Engine

Mit dem **Hardware Accelerator** wird der Vorgang zum Scannen und Auffinden von Virus-Signaturen im e-mail- und webbasierten Datenverkehr um ein vielfaches beschleunigt. Die Karte nutzt dafür eine eigenständige Version der leistungsstarken Open Source Software.
Sie schalten den *Hardware Anti-Virus Scanner* durch einen Klick auf die Schaltfläche **Enable** ein.

Tipp:

Falls auf Ihrem System der *Hardware Accelerator* installiert ist, können Sie zur Verbesserung der Rechner-Performance den *Open Source Software Anti-Virus Scanner* für den Proxy *HTTP* deaktivieren.

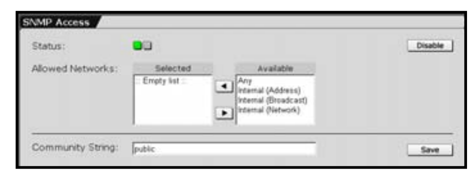
Astaro Engine

Bei der **Astaro AV Engine** handelt es sich um eine technisch ausgereifte Lösung. Sie erkennt die verschiedenartigsten E-Mail- und Webbasierten Viren, Würmer und andere Malware die nur durch heuristische Analysen entdeckt werden können.
Sie schalten den *Software Anti-Virus Scanner* durch einen Klick auf die Schaltfläche **Enable** ein.

Open Source Engine

Die **Open Source Engine** nutzt ein Verzeichnis mit bereits entdeckten Viren. Die Codes in den Datenpaketen werden mit denen der bereits entdeckten Viren verglichen. Falls ein Bereich des Codes mit bereits bekannten Viren übereinstimmt, werden diese dann durch die geeignete Maßnahme gefiltert.
Sie schalten den *Software Anti-Virus Scanner* durch einen Klick auf die Schaltfläche **Enable** ein.

5.1.6. SNMP



Das **Simple Network Management Protocol** (**SNMP**) dient zur Überwachung und zum Managen des lokalen Netzwerks. Der Administrator kann mit *SNMP* schnell den Zustand der Netzwerkgeräte, wie z. B. die Anzahl und Konfiguration der Netzwerk-Interfaces, die übertragene Datenmenge, die laufenden Prozesse und die Auslastung der Festplatten abfragen. Über den augenblicklichen Zustand hinaus sind Trends und Zeitreihen interessant. Sie geben einen tiefen Einblick in die Funktion eines Netzwerks - in der Historie lassen sich oft Engpässe in ihrer Entstehung beobachten und beheben, bevor sie zum Problem werden.

Im Fenster **SNMP Access** stellen Sie die Berechtigungen für den Zugriff auf den *SNMP*-Dienst ein. Die Benutzer aus den eingestellten Netzwerken können dann mit Read-only-Berechtigung Abfragen an den SNMP-Server auf dem Internet-Sicherheitssystem ausführen.

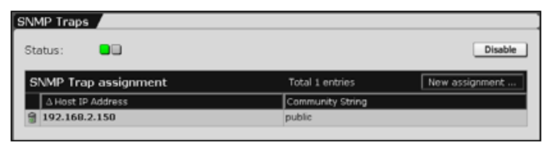


Sicherheitshinweis:

Der **SNMP**-Datenverkehr (Protokoll Version 2) zwischen dem Internet-Sicherheitssystem und dem Netzwerk ist unverschlüsselt.

Zugang auf SNMP-Server erlauben:

1. Schalten Sie die Funktion **SNMP Access** durch einen Klick auf die Schaltfläche **Enable** ein.
2. Wählen Sie im Auswahlfeld **Allowed Networks** die Netzwerke aus, von denen auf den *SNMP*-Server zugegriffen werden darf.
3. Tragen Sie in das Eingabefeld den **Community String** ein.
4. Speichern Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.



Im Fenster **SNMP Traps** können Sie einen *Trap-Server* definieren, an den für die Systemadministration relevante Benachrichtigungen als **SNMP Traps** abgeschickt werden. Zur Erkennung dieser *Traps* wird eine spezielle SNMP-Überwachungs-Software benötigt.

Die Benachrichtigungen, die als *SNMP Trap* abgeschickt werden, enthalten die **Objekt ID** (**OID**) der Astaro AG. Die *OID* für Benachrichtigungsereignisse (1500), die Einstufung der Benachrichtigung (DEBUG = 0, INFO = 1, WARN = 2, CRIT = 3) und der entsprechende Fehler-Code (000 bis 999) werden angehängt.

Beispiel: Die Notification INFO-354: Intrusion Protection Pattern Up2Date succeeded hat in diesem Fall die *OID* 1.3.6.1.4.1.9789.1500.1.354 und bekommt den folgenden String zugewiesen: [<HOST>][INFO][354]. Für den Platzhalter <HOST> wird der Hostname des Sicherheitssystems angezeigt.

Trap-Server zuweisen:

1. Schalten Sie die Funktion **SNMP Traps** durch einen Klick auf die Schaltfläche **Enable** ein.

   Die Statusampel zeigt Grün und ein erweitertes Eingabefenster wird geöffnet.

2. Klicken Sie in der Tabelle **SNMP Tap Assignment** auf die Schaltfläche **New Assignment**.

3. Klicken Sie in der Spalte **Host IP Address** auf die neue Zeile.

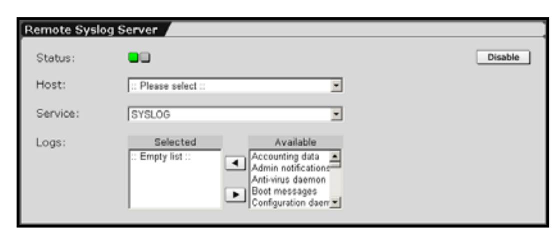
   Anschließend öffnet sich ein Editierfenster.

4. Tragen Sie in das Eingabefeld die IP-Adresse des Servers ein und speichern Sie die Eingabe durch einen Klick auf die Schaltfläche **Save**.

5. Klicken Sie in der Spalte **Community String** auf den Eintrag **public** und tragen Sie in das Eingabefeld den *Community String* ein.

Die neue Zuweisung wird anschließend sofort übernommen.

5.1.7. Remote Syslog Server



Mit dieser Funktion können Sie die Protokolle (Logs) des Internet-Sicherheitssystems an verschiedene Hosts weiterleiten. Dies ist besonders dann sinnvoll, wenn Sie die Log-Dateien verschiedener Systeme auf einzelne Hosts zusammenführen wollen. Per Default ist die Funktion ausgeschaltet.
Auf dem ausgewählten Host muss ein zum Protokoll *Syslog* kompatibler *Logging Daemon* laufen.

Achtung:

Wählen Sie im Menü **System/Remote Syslog Server** als Zieladresse (Host) kein Interface des Sicherheitssystems, z. B. eth0 aus.

Host: Wählen Sie im Drop-down-Menü einen Host aus, der die entsprechende Log-Daten empfangen soll. Nach Auswahl eines Hosts wird die Weiterleitung der ausgewählten Log-Daten ohne eine weitere Meldung gestartet.
Die dazu nötige Definition des Hosts (Netzwerk mit Netzmaske 255.255.255.255) nehmen Sie im Menü **Definitions/Networks** vor. Das Definieren von Netzwerken wird ausführlich in Kapitel 5.2 ab Seite 134 beschrieben.

Service: Per Default ist das Protokoll **Syslog** eingestellt. Sie können in diesem Drop-down-Menü auch den Dienst (bzw. Port) einstellen, der auf dem Remote Server verwendet wird.

Logs: In diesem Auswahlfeld können die Log-Dateien ausgewählt werden, die an den Remote Host gesendet werden sollen.

5.1.8. User Authentication

Benutzerauthentifizierung (User Authentication) ist auf diesem Internet-Sicherheitssystem mit den Proxydiensten HTTP, SMTP und SOCKSv5 möglich. Es kann festgelegt werden, welcher Benutzer diese Proxydienste in Anspruch nehmen darf. Die Benutzer-Accounts können lokal auf dem System im Menü **Definitions/Users** angelegt werden. Es können aber auch externe Benutzer-Datenbanken abgefragt werden. Unterstützt werden die Authentifizierungsmethoden **RADIUS**, **SAM** (Windows NT/Windows 2000/XP-Server), **Microsoft Active Directory**, die Domain-Anbindungs-Methode von **NTML** und **OpenLDAP**. Dies kann von Vorteil sein, wenn bereits eine Benutzerdatenbank auf einem solchen Server vorhanden ist, und die Benutzer somit nicht noch einmal auf dem Internet-Sicherheitssystem eingetragen werden müssen.

Wichtiger Hinweis:

Bitte beachten Sie, dass verschiedene Authentifizierungsmethoden nicht zur selben Zeit unterstützt werden können.

In MS-Windows-basierten Netzwerken verwaltet der **Domain Controller** (**DC**) für eine Client-Gruppe den Zugang auf die zur Verfügung stehenden Ressourcen (z. B. Applikationen, Drucker, etc.) Der Benutzer muss sich nur in der Domain anmelden um den Zugang zu diesen Ressourcen zu erhalten. Die aktuellen Betriebssysteme eines *Domain Controllers* sind **Microsoft Windows 2000 Server** und **2003 Server** und enthalten den **Microsoft**-eigenen Verzeichnisdienst **Active Directory** (**AD**).

Ein Verzeichnisdienst stellt in einem Netzwerk zentralisiert Informationen zu Geräten (Devices), Diensten (Services) und den zugriffsberechtigten Benutzern (authorized Users) zur Verfügung. Für die Windows-Nutzer verteilt der Verzeichnisdienst Account-Informationen, Rechte, Profile und die Policy. Bei Verwendung einer Authentifizierungsmethode mit *Active Directory* erfolgt bei entsprechender Konfi-

guration die Authentifizierung, z. B. vor dem Zugriff auf einen *Dienst* (*Service*) nicht mehr über das Sicherheitssystem, sondern über den *Active-Directory*-Server.

Die Authentifizierung des Clients bei Anfragen an einen Proxydienst muss durch Benutzernamen und Passwort erfolgen. Auf diese Weise wird die Authentifizierung personenbezogen (User) und nicht IP-bezogen durchgeführt. Dies ermöglicht ein personenbezogenes **Accounting** im HTTP-Proxy Zugangsprotokoll.

Proxydienste und Authentifizierungsmethoden

Die Proxydienste **HTTP**, **SMTP** und **SOCKSv5** können so konfiguriert werden, dass sie alle Clients (auf IP-Adressen basierend) oder nur Clients mit einem gültigen Benutzernamen und Passwort (Benutzerauthentifizierung) akzeptieren. Wenn Sie **User Authentication** aktivieren, müssen Sie mindestens eine Methode für Ihr System auswählen, um die angefragten Berechtigungsnachweise zu bewerten. Ansonsten können Sie den Proxydienst nicht benutzen.

Das Sicherheitssystem unterstützt Benutzerauthentifizierung mit ...

- einem Novell-eDirectory-Server
- einem RADIUS-Server
- einer NT SAM Benutzer-Basis
- eine Active Directory/NT Domain Membership
- einem LDAP-Server
- einer lokalen Benutzerdatenbank im WebAdmin

Die fünf Benutzerdatenbanken können nacheinander abgefragt werden.

5.1.8.1. Local Users

Um die Sicherheit für das Sicherheitssystem und somit auch für das interne Netzwerk zu erhöhen unterliegt die Zusammensetzung und die Länge des Passworts den nachfolgend aufgeführten Restriktionen. Das Passwort wird vom Sicherheitssystem nur übernommen, wenn diese Bestimmungen erfüllt sind:

- eine Mindestlänge von acht Zeichen
- mindestens ein kleingeschriebener Buchstabe
- mindestens ein großgeschriebener Buchstabe
- mindestens eine Zahl
- mindestens ein nicht-alphanumerisches Zeichen (innerhalb der ASII-Tabelle, Zeile 32 bis 126)

Die Restriktionen für die Passwörter sind nur für neu Installierte Sicherheitssysteme ab Version 6.105 gültig oder treten in Kraft falls ab der Version 6.105 die Aktion **Passwort Reset** oder **Factory Reset** durchgeführt wurde.



Force Complex Passwords: Um sicherzustellen, dass bei Neuinstallationen möglichst sichere Passwörter gemäß den Definitionen der *Common Criteria* gesetzt werden, ist diese Funktion zu Beginn eingeschaltet. Wenn diese Funktion ausgeschaltet wird, werden vom Sicherheitssystem alle Passwörter akzeptiert.

Hinweis:

Wenn Sie auf dem Sicherheitssystem im **Common Criteria Mode** diese Funktionen ausschalten, arbeitet das Sicherheitssystem nicht mehr mit der **Bewerteten Konfiguration**. Der *Common Criteria Mode* wird in diesem Fall automatisch deaktiviert.

5.1.8.2. Novell eDirectory

Novell eDirectory – Novell Directory Service 8.7.1 - ist ein auf X.500 basierender Verzeichnisdienst zur Verwaltung von Benutzern, Zugriffsrechten und anderen Netzwerkressourcen. Novell stellt den Verzeichnisdienst für die Plattformen Netware ab Version 5, MS Windows NT/2000, Linux, Solaris und demnächst auch für HP-UX zur Verfügung.

Novell eDirectory-Server einstellen:

Auf dem Stand-alone-LDAP-Server muss ein Benutzer eingerichtet sein, der die Leserechte für das gesamte Verzeichnis hat.



Sicherheitshinweis:

Stellen Sie sicher, dass dieser Benutzer **nur** die Leserechte bekommt.

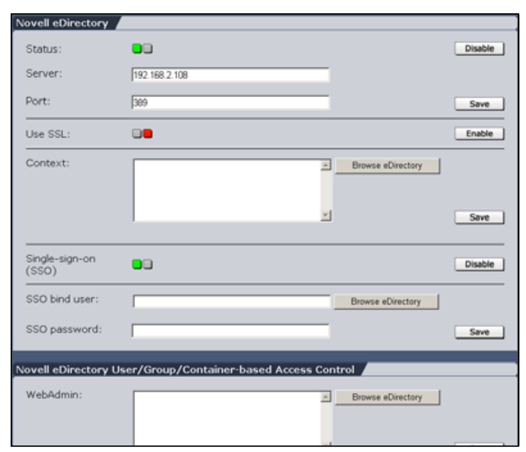
Bei **Novell eDirectory (NDS8)** sollte der Abfrage-Typ **groupMembership** verwendet werden, da sich ein bereits vollständig eingerichteter Verzeichnisdienst einfach erweitern lässt.
Das Verzeichnis kann wiederum um selbstdefinierte Attribute erweitert werden. Diese Attribute, die für jeden Benutzer einzeln auf dem Directory-Server gesetzt werden müssen, geben durch den Wert oder den Inhalt Auskunft welche Berechtigungen dem Benutzer zugewiesen wurden.
Für die Konfiguration des Novell eDirectory-Servers benötigen Sie die **Novell ConsoleOne**.

Die Verwaltung des Novell-eDirectory-Servers wird ausführlich in der zugehörigen Dokumentation beschrieben. Sie erhalten die Dokumentation unter der Internetadresse:

http://www.novell.com/documentation/lg/edir87/index.html

Führen Sie anschließend die Einstellungen am Internet-Sicherheits-system durch.

Novell eDirectory auf Sicherheitssystem einstellen:



Auf dem Novell-eDirectory-Server muss ein Benutzer eingerichtet sein, der die Leserechte für das gesamte Verzeichnis hat.

Um die nötigen Einstellungen auf dem Internet-Sicherheitssystem durchzuführen, benötigen Sie den **Distinguished Name (DN)** dieses Benutzers und die IP-Adresse des Stand-alone-LDAP-Servers.



Sicherheitshinweis:

Stellen Sie sicher, dass der Benutzer **nur** die Leserechte für den Stand-alone-LDAP-Server bekommt.

1. Öffnen Sie im Verzeichnis **System** das Menü **eDirectory**.

2. Schalten Sie die Funktion im Fenster **Novell eDirectory** durch einen Klick auf die Schaltfläche **Enable** bei **Status** ein.

   Server: Tragen Sie in das Eingabefeld die IP-Adresse des Stand-alone-LDAP-Servers ein.

   Port: Tragen Sie in das Eingabefeld den TCP Port ein. Der Standard-Port 636 ist bereits eingetragen.

   Context: Definieren Sie in der Kontrollliste die Gruppe des Benutzers aus dem Verzeichnisdienst, der hier authentisiert werden soll - z. B. bei Verwendung der LDAP-Schreibweise durch den

gesamten **Distinguished Name (DN)** des Benutzers.
Beispiel: **DN**: cn=administrator, o=our_organisation

Hinweis:

Novell-Directory-Service-Gruppen können entweder durch *Common Name (CN)* der Gruppe oder durch den gesamten *Distinguished Name (DN)* in der LDAP-Schreibweise definiert werden. Als Trennsymbol wird das Komma verwendet. Der Punkt wird hier zur Abgrenzung nicht unterstützt.

---

3. Falls Sie die Verbindung zum LDAP-Server mit dem SSL-Standard verschlüsseln möchten, schalten Sie die Funktion in der Zeile **Use SSL** durch einen Klick auf die Schaltfläche **Enable** ein.

   Durch die Verschlüsselung haben Sie die Möglichkeit die Authentisierung mittels *Novell eDirectory* auch über öffentliche Netzwerke zu nutzen.

4. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

Single Sign-on (SSO): Ab Version 6.2 enthält das Sicherheitssystem den *Single-Sign-On*-Mechanismus für den Verzeichnisdienst Novell eDirectory. Die Authentifizierung für den Internetzugang erfolgt damit einmalig - der Benutzer muss sich nicht jedes Mal vor der Nutzung des Internets mit **Benutzernamen** und **Passwort** anmelden.

Sobald die Authentifizierung erstmalig durchgeführt wurde steht benutzerbasierend die gesamte Funktionalität der **Web Security Subscription** zur Verfügung - dies beinhaltet *Virus Protection*, *Spam Protection* und *Phishing Protection*. Eine weitere Authentifizierung auf Browser Level ist nicht mehr nötig.

Diese Implementierung erleichtert in Verbindung mit den Novell-eDirectory-Diensten die Administration des Sicherheitssystems und steigert erheblich die Sicherheit des Netzwerks.

Single-Sign-On-Mechanismus einschalten:

1. Klicken Sie in der Zeile **Single-Sign-on (SSO)** auf die Schaltfläche Enable.

   Die Statusampel zeigt grün und ein erweitertes Eingabemenü wird angezeigt.

2. Führen Sie die folgenden Einstellung durch:

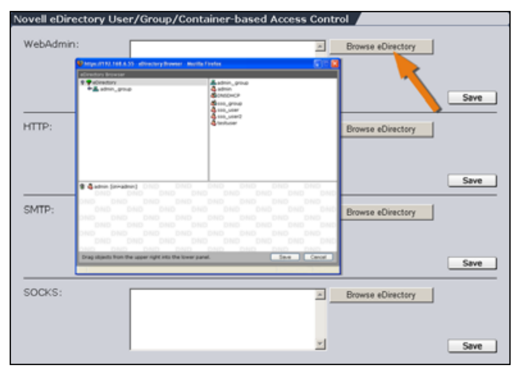
   SSO bind user: Tragen Sie in das Eingabefeld den Benutzernamen ein.

   Um die Benutzer authenfizieren zu können, müssen die Zugangsdaten ausreichend Rechte für alle relevanten Benutzerobjektinformationen vom Novell-eDirectory-Server beinhalten.

   SSO password: Tragen Sie in das Eingabefeld das Passwort für den *SSO Bind User* ein.

Der SSO-Mechanismus ist nun aktiviert.

Novell eDirectory User/Group/Container-based Access Control



Die Novell-eDirectory-Gruppen können genutzt werden, um die Zugangskontrolle für die verschiedenen Authentisierungs-Clients zu verwalten. Definieren Sie in der entsprechenden Kontrollliste die Gruppe des Benutzers aus dem Verzeichnisdienst, der hier authentisiert werden soll.

Ab dem Sicherheitssystem *Version 6.2* ist im Menü bei jedem Dienst ein **eDirectory Browser** mit der Struktur des Verzeichnisdienstes enthalten. Mit Hilfe dieses eDirectory Browsers ist der Administrator in der Lage über das Sicherheitssystem *Benutzer* (*Users*), *Benutzergrup-*

pen (*User Groups*) oder *Container* (*Containers*) auszuwählen und sie den **Zugangskontrollprofilen** oder den **Web Security** Policies zuzuordnen. Mit dem *eDirectory Browser* muss der Administrator keine aufwendigen *LDAP*-Regeln mehr definieren und keine *LDAP Distinguished Names* (*DNs*) mehr verwalten.

Im linken Bereich des Browser-Fensters wird die Struktur des Verzeichnisbaums angezeigt. Im rechten Fenster können Sie die *Benutzer* (*Users*), *Benutzergruppen* (*User Groups*) oder *Container* (*Containers*) mit der Maus auswählen und in das untere Fenster ziehen.
Die ausgewählten Komponenten können durch einen Klick auf das *Papierkorb*-Symbol ( ) wieder *gelöscht* werden.

Um die Änderung zu speichern, klicken Sie anschließend auf die Schaltfläche **Save**. Durch einen Klick auf die Schaltfläche **Cancel** werden die Änderungen wieder verworfen.

Die neuen Einstellungen werden in das Menü **Context** kopiert. Die Änderungen im *eDirectory Browser* können auch manuell im Menü **Context** durchgeführt werden.

Die neuen Einstellung werden durch einen Klick auf die Schaltfläche **Save** vom System übernommen.

Die möglichen Dienste sind:

WebAdmin: Überwacht den Zugang auf das Konfigurationstool *WebAdmin*.

HTTP: Überwacht die Profilzuweisung zur Nutzung des HTTP-Proxy.

SMTP: Überwacht die SMTP-Authentisierung, wenn z. B. für die Verbindung die TLS-Verschlüsselung eingeschaltet ist.

SOCKS: Ermöglicht Client-Server-Applikationen die transparente Nutzung der Dienste einer Netzwerk-Firewall. Die Benutzerauthentisierung wurde innerhalb des SOCKSv5-Protokolls durchgeführt.

5.1.8.3. RADIUS

RADIUS steht für **Remote Authentication Dial In User Service** und ist ein Protokoll, mit dem z. B. ein ISDN-Router Informationen für die Benutzerauthentifizierung von einem zentralen Server abfragen kann. Neben den reinen Benutzerinformationen für die Authentifizierung verwaltet RADIUS auch technische Informationen, die für die Verständigung des Zugangssystems mit dem Endgerät des Anrufers nötig sind. Dazu gehören z. B. die verwendeten Protokolle, IP-Adressen, Telefonnummern, Time-outs, Routen etc. Zusammen bilden sie ein Benutzerprofil, das in einer Datei oder Datenbank auf dem RADIUS-Server gespeichert wird.
Neben der Authentifizierung von DialUp-Usern kann **RADIUS** aber auch als generisches Authentifizierungsprotokoll verwendet werden.

Das Protokoll ist sehr flexibel und die RADIUS-Server sind für alle Betriebssysteme eingeschlossen Microsoft Windows NT/2000 verfügbar. Die RADIUS-Implementierung dieses Internet-Sicherheitssystems ermöglicht Ihnen die Zugriffsrechte auf Proxy- und Benutzerbasis zu konfigurieren.

Bevor Sie **RADIUS**-Authentication einstellen können, benötigen Sie einen RADIUS-Server in Ihrem Netzwerk. Da die Passwörter in Klartext übertragen werden, empfehlen wir jedoch, den RADIUS-Server ausschließlich in einer geswitchten Umgebung zu verwenden.

Im folgenden Abschnitt wird als Beispiel detailliert das Einrichten von Microsofts IAS (RADIUS-Server für MS Windows NT und 2000) beschrieben. Falls Sie einen anderen RADIUS-Server verwenden, benötigen Sie die folgenden Informationen, um den Betrieb mit der Benutzerauthentifizierung des Internet-Sicherheitssystems zu ermöglichen.

Die Authentifizierungsanfrage enthält drei gesetzte Felder:

- Benutzername
- Passwort in Klartext (PAP)
- Proxyart (String **http**, **smtp** oder **socks**) im Feld **NAS-Identifier**

Der RADIUS-Server muss anhand dieser Informationen entscheiden, ob der Zugriff auf den Proxy bewilligt wird, und eine entsprechende Antwort zurückliefern.

Microsofts IAS RADIUS-Server einstellen:

IAS wird mit allen Microsoft-Windows-2000-Server-Versionen ausgeliefert, ist aber standardmäßig meist nicht installiert. Für Microsoft Windows NT4 ist **IAS** Bestandteil von **NT4 Option Pack** und ist ohne Aufpreis erhältlich. Die MS Windows NT4 IAS-Version hat weniger Features als die 2000er-Version, jedoch reicht diese für die gebräuchlichen Authentifizierungs-Einstellungen dieses Sicherheitssystems vollkommen aus.

1. Installieren Sie den **IAS**-Dienst, falls er nicht bereits installiert ist.
2. Legen Sie für jeden Proxy, der verwendet werden soll, eine Benutzergruppe an.

   Tipp:

   Benennen Sie die Gruppe entsprechend des zugeordneten Proxydienstes. Die Gruppe für den HTTP-Proxy könnte z. B. **HTTP-Proxybenutzer** lauten.

3. Nun ordnen Sie dieser Gruppe alle Benutzer zu, die in der Lage sein sollen, den entsprechenden Proxy zu benutzen.
4. Stellen Sie sicher, dass bei allen Benutzern in diesen Gruppen das Benutzerflag **Einwahlzugriff auf das Netzwerk erlauben** aktiviert ist.

Diese Einstellung finden Sie in den Benutzereigenschaften. MS Windows NT/2000 benötigt dieses Flag, um RADIUS-Anfragen positiv zu beantworten.

5. Öffnen Sie das Verwaltungsprogramm für den **IAS**-Dienst.

6. Fügen Sie einen Client hinzu. Dazu müssen Sie folgende Angaben machen:

   Beliebiger Client-Namen: Tragen Sie hier den **DNS**-Namen Ihres Internet-Sicherheitssystems ein.

   Protokoll: Wählen Sie hier **RADIUS** aus.

   IP-Adresse des Clients: Dies ist die interne IP-Adresse Ihres Internet-Sicherheitssystems.

   Client Vendor: Tragen Sie hier **RADIUS Standard** ein.

   Shared Secret: Tragen Sie ein beliebiges Passwort ein. Dieses Passwort benötigen Sie später zur Konfiguration des RADIUS-Servers im Konfigurationstool **WebAdmin**.



Sicherheitshinweis:

Für das **Shared Secret** werden nur Passwörter bestehend aus alphanumerischen sowie Minus- und Punkt-Zeichen unterstützt. Sonderzeichen, z. B. %!#_{} sind nicht möglich.

7. Wechseln Sie zum Menü **RAS-Richtlinien**.
   Hier ist eine Standardrichtlinie eingetragen. Wenn Sie **IAS** nur für das Internet-Sicherheitssystem verwenden wollen, können Sie diese löschen.

   Tragen Sie nun für jeden Proxy eine Richtlinie ein. Auf diese Weise können Sie den Namen entsprechend wählen, z. B. HTTP-Zugriff.

Fügen Sie zwei Bedingungen hinzu:

1. Bedingung: Das Feld NAS-Identifier muss einem String laut folgender Tabelle entsprechen.

Proxytyp	NAS Identifier entspricht String
HTTP	http
L2TP over IPSec	l2tp
PPTP	pptp
SOCKS	socks
SMTP	smtp
WebAdmin Access	webadmin
Surf Protection	“Profilname”

2. Bedingung: Die Windows-Gruppe des zugreifenden Benutzers muss der in Schritt 2 angelegten Benutzergruppe entsprechen.

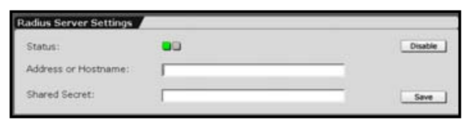
Nur wenn vom Benutzer beide Bedingungen erfüllt werden, wird der Zugriff erlaubt.

8. Stellen Sie das Profil so ein, dass nur eine verschlüsselte Verbindung erlaubt wird, indem Sie im Register **Verschlüsselung** die Funktion **Keine Verschlüsselung** ausschalten.

9. Stellen Sie das Profil so ein, dass eine *unverschlüsselte Authentifizierung (CHAP)* erlaubt wird, indem Sie im Register **Authentifizierung** die Funktion **verschlüsselte Authentifizierung (CHAP)** ausschalten.
Belassen Sie bei allen anderen Profil-Einstellungen die voreingestellten Werte.

10. Starten Sie das Konfigurationstool **WebAdmin** und öffnen im Verzeichnis **System** das Menü **User Authentication**.

11. Schalten Sie die Funktion im Fenster **RADIUS Server Settings** durch einem Klick auf die Schaltfläche **Enable** bei **Status** ein (Statusampel zeigt Grün).



Address or Hostname: Tragen Sie hier die IP-Adresse oder den Hostnamen des RADIUS-Servers ein.

Shared Secret: Tragen Sie hier das Passwort **Shared Secret** aus Schritt 6 ein.

12. Speichern Sie die Eingabe durch einen Klick auf die Schaltfläche **Save**.

13. Öffnen Sie das Menü des entsprechenden Proxys, bei dem Benutzerauthentifizierung mittels RADIUS erfolgen soll.

14. Falls **User Authentication** noch ausgeschaltet ist (Statusampel zeigt Rot), aktivieren Sie diese, indem Sie auf die Schaltfläche **Enable** klicken.

    Authentication Methodes: Wählen Sie in diesem Auswahlfeld RADIUS aus.

15. Bestätigen Sie nun Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

Die Benutzerauthentifizierung per **RADIUS** ist nun aktiviert.
Im Microsoft Windows NT/2000 **Event Log** protokolliert anschließend der IAS-Server jeden Zugriff auf den Proxyserver.

Um ein schnelles Volllaufen des Event-Logs zu verhindern, speichert das Internet-Sicherheitssystem die vom RADIUS-Server gelieferten Daten für fünf Minuten. Das bedeutet allerdings auch, dass sich Änderungen an der Benutzerdatenbank gegebenenfalls erst nach maximal fünf Minuten bemerkbar machen.

Achtung:

Das Sicherheitssystem sendet Anfragen über den UDP-Port 1812.

5.1.8.4. SAM – NT/2000/XP

Bei dieser Authentifizierungsmethode wird zur Bewertung der Anfragen ein *MS Windows NT/2000 Domain Controller* oder ein *Stand-alone-Server* verwendet. Viele Unternehmen verwenden bereits MS Windows NT/2000-Netzwerke, die auf dem MS Windows NT/2000 Active Directory-Domain-Konzept basieren.
Der Vorteil von SAM ist, dass es sehr einfach zu konfigurieren ist, wenn auf dem Netzwerk schon ein **Primary Domain Controller (PDC)** oder ein einfacher Server mit Benutzerdatenbank läuft.
Der Nachteil ist, dass bei diesem Modell nicht zwischen verschiedenen Benutzergruppen unterschieden werden kann. Sie können entweder alle Benutzer einer SAM-Datenbank für einen bestimmten Proxy freischalten oder keinen.

SAM – NT/2000/XP einstellen:



Um diese Authentifizierungsmethode zu verwenden, benötigen Sie einen Microsoft Windows NT- oder 2000-Server in Ihrem Netzwerk, der die Benutzer-Daten enthält. Dies kann entweder ein Primary Domain Controller (PDC) oder ein selbständiger Server sein.

Dieser Server hat einen NETBIOS-Namen (der NT/2000 Servername) und eine IP-Adresse.

1. Öffnen Sie im Verzeichnis **System** das Menü **User Authentication**.

2. Schalten Sie die Funktion im Fenster **SAM (NT/2000/XP) Server Settings** durch einem Klick auf die Schaltfläche **Enable** bei **Status** ein.

   PDC Name: Tragen Sie in dieses Eingabefeld den Namen des Domain-Controllers ein.

Da ab Microsoft Windows 2000 diese Namen auch offizielle **DNS**-Namen sind, unterstützen wir nur Namen bestehend aus alphanumerischen sowie Minus- und Punkt-Zeichen.
Sonderzeichen, z. B. %!#_{} werden als Fehler gewertet.

PDC Address: Tragen Sie in dieses Eingabefeld die IP-Adresse des Domain-Controllers ein.

BDC Name: Wenn Sie einen Backup Domain Controller verwenden, tragen Sie in dieses Eingabefeld den Namen ein. Falls Sie keinen BDC verwenden, tragen Sie hier den Namen des PDC ein.

BDC Address: Tragen Sie in dieses Eingabefeld die IP-Adresse des Backup Domain Controllers ein. Falls Sie keinen BDC verwenden, tragen Sie hier die IP-Adresse des PDC ein.

NT4 Domain: Tragen Sie hier den Namen Ihrer MS Windows NT/2000-Domain ein.
Erlaubte Zeichen sind: Das Alphabet, das Minus-Zeichen (-) und Unterstrich (_).

Hinweis:

Dies ist keine Internet-Domain, wie etwa Firma.de, sondern ein einfacher Bezeichner, z. B. **Intranet**. Falls Sie das Microsoft Domain-Konzept nicht benutzen, sondern nur einen einfachen Server haben, tragen Sie hier den NETBios-Namen des Servers ein. Dies entspricht dem Eintrag im Eingabefeld **PDC Name**.

---

3. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.



Sicherheitshinweis:

Für das **Shared Secret** werden nur Passwörter bestehend aus alphanumerischen sowie Minus- und Punkt-Zeichen unterstützt. Sonderzeichen, z. B. %!#_{} sind nicht möglich.



Sicherheitshinweis:

Wenn Sie SAM-Authentifizierung verwenden, sollten Sie den **Guest**-Account Ihrer Windows-Domain deaktivieren, da sonst alle Benutzer/Passwort-Kombinationen als gültig angesehen werden!

5.1.8.5. Active Directory/NT Domain Membership

Bei dieser Authentifizierungsmethode wird das Protokoll **NTLM** verwendet. **NTLM** steht für **New Technology LAN Manager** und ist eine Weiterentwicklung des LAN-Managerprotokolls **LM** zur Benutzerauthentifizierung in Windows-Netzwerken. Das Challange-Response basierte Protokoll *NTLM* ist standardmäßig auf den Betriebssystemen MS Windows 2000 und 2003 Server enthalten. Der Squid-Proxy kann mit diesem Protokoll Benutzer authentifizieren.

Bei dieser Authentifizierungsmethode wird zur Bewertung der Anfragen ein **MS Windows NT/2000 Domain Controller (DC)** verwendet. Weitere Informationen zu *Domain Controller (DC)* erhalten Sie in der Einleitung zum Menü **User Authentication** auf Seite 83.

Die Authentifizierungmethode mit *NTML* unterstützt neben *RADIUS* ebenfalls die Fern-(Remote)-Benutzerauthentifizierung. Die Methode mit *NTLM* hat allerdings gegenüber von *RADIUS* den Vorteil, dass sich der Benutzer aufgrund des **Single-Sign-On**-Mechanismus nicht jedesmal vor der Nutzung des Internets mit **Benutzernamen** und **Passwort** anmelden muss.

Die Funktionsweise der Domain-Anbindungs-Methode von *NTML* unterscheidet sich komplett von den drei anderen Authentifizierungsmethoden auf diesem Sicherheitssystem. Die Authentifizierung mit *NTML* wird in **MS-Windows**-Umgebungen in der Regel für Clients eingesetzt, die den Browser **Internet Explorer** nutzen. Allerdings sind auch Systeme mit Clients erfolgreich im Einsatz, auf denen die Browser **Firefox** oder **Mozilla** (z. B. Mozilla 1.6) genutzt werden.

Hinweis:

Damit die Anbindung des Internet-Sicherheitssystems an die **Domain** zustande kommt, muss einer der **Domain Controller (DC)** für diese *Domain* innerhalb des System-Broadcast-Bereichs liegen. Die Authentifizierung mit **NTLM** kann zurzeit nur für den HTTP-Proxy genutzt werden um *Single-Sign-On*-Anmeldungen für *Internet-Explorer*-Clients durchzuführen!

Der Begriff **Single Sign-On** (**SSO**) wird im Allgemeinen für ein einmaliges, zentrales Anmelden eines Benutzers in einer IT-Struktur verwendet. Dies hat den Vorteil, dass der Benutzer seine Kennungsdaten nur einmal eingeben muss und dann an allen zentral angeschlossenen Diensten authentifiziert ist. Dies ermöglicht es in einem Unternehmen eine einheitliche Benutzer- und Rechtestruktur durchzusetzen.

Bei der Konzeption einer zentralen, einmaligen Authentifizierung, der auf bestehende Infrastrukturen aufbauen soll, müssen eine Reihe von Anforderungen erfüllt werden:

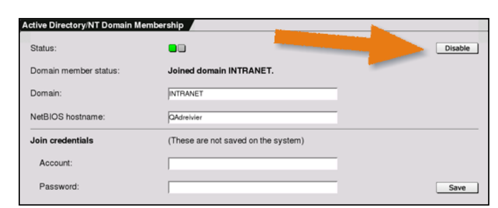
- Zentrale Administration: Benutzerauthentifizierungsdaten werden nur an einer Stelle gepflegt
- Einfache Benutzbarkeit: Daten werden konsistent und nicht doppelt gehalten, d. h. nur ein Passwort für sämtliche Dienste
- Sicherheit: Passwörter sind nicht für Angreifer lesbar

Der Vorteil des letzteren ist, dass die Daten im hier vorgestellten Konzept nie unverschlüsselt über Netzwerke übertragen werden und einer bestimmten Verfallsdauer unterliegen. Dies macht einen Brute-Force-Angriff auf die verschlüsselten Daten nahezu unmöglich.

Active Directory / NT Domain Membership einstellen:

1. Öffnen Sie im Verzeichnis **System** das Menü **User Authentication**.

2. Schalten Sie die Funktion im Fenster **Active Directory / NT Domain Membership (NT / 2000 / XP) Server Settings** durch einem Klick auf die Schaltfläche **Enable** bei **Status** ein.



Wenn Sie **NTLM Domain Membership** hier später wieder ausschalten, wird das Sicherheitssystem nicht sofort bei der Domain abgemeldet – dies muss auf dem Domain Controller durchgeführt werden.

Domain Member Status: Nach einer erfolgreichen Anmeldung wird hier die Meldung **Joined domain „Domain-Name“** angezeigt.

Domain: Tragen Sie hier den Namen Ihrer MS Windows NT/ 2000-Domain ein.
Erlaubte Zeichen sind: Das Alphabet, das Minus-Zeichen (-) und Unterstrich (_).

Hinweis:

Dies ist keine Internet-Domain, wie etwa Firma.de, sondern ein einfacher Bezeichner, z. B. **Intranet**.

NetBIOS Hostname: Tragen Sie hier den *NetBIOS Hostname* ein, der in der Domain für das Sicherheitssystem verwendet werden soll. Sie können sich einen beliebigen Namen ausdenken. Dieser hat keinerlei Signifikanz. Jedoch sollten Sie um Konflikte zu vermeiden, einen Namen verwenden, der in der Domain noch nicht verwendet wird.

Achtung:

Um Konflikte zu vermeiden, tragen Sie hier nicht einen Hostnamen ein, der bereits auf einem anderen System eingesetzt wird - insbesondere nicht den Hostnamen des Domain Controller!

Account: Tragen Sie in das Eingabefeld den *Account*-Namen ein, der auch die Rechte für die Anbindung von Clients an eine Domain enthält. In der Regel ist dies der Administrator. Dieser Name wird nur zur Anbindung an die Domain verwendet und wird nicht auf dem Sicherheitssystem gespeichert!

Passwort: Tragen Sie in das Eingabefeld das *Passwort* zum *Account*-Namen ein. Dieses Passwort wird ebenso nur zur Anbindung an die *Domain* verwendet und wird nicht auf dem Sicherheitssystem gespeichert!

Clear Authentication Cache: Diese Funktion kann verwendet werden, wenn Sie bei Ihrer bestehenden MS Windows NT/2000-Domain z. B. neue Benutzer hinzugefügt oder die Gruppenzugehörigkeit bestehender Benutzer verändert haben. Wenn Sie den *Authentication Cache* nicht leeren, kann es bis zu 24 Stunden dauern bis Ihre Änderungenauf dem Sicherheitssystem wirksam werden.

3. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

Sobald die Anbindung des Sicherheitssystems an die **Domain** erfolgreich durchgeführt wurde, erscheint bei **Domain Member Status** die Bestätigung.

5.1.8.6. LDAP Server

LDAP steht für **Lightweight Directory Access Protocol** und ist ein Kommunikationsprotokoll das den Transport und das Format von Nachrichten definiert, die von einem Client für den Zugriff auf einen X.500-konformen Verzeichnisdienst verwendet werden. Das Protokoll spezifiziert somit die Art des Zugriffs auf einen solchen Verzeichnisdienst.

Bei diesem Internet-Sicherheitssystem wird das Protokoll **LDAP** zur Benutzerauthentifizierung eingesetzt, indem mit Hilfe von Stand-alone-LDAP-Servern Verzeichnisse nach einem Benutzer mit einer bestimmten Gruppenzugehörigkeit oder mit bestimmten Attributen abgefragt werden.
Das System unterstützt die Stand-alone-LDAP-Server **Microsoft Active Directory** und **Novell eDirectory** sowie LDAP-Server, die auf der Open-Source-Implementation von **OpenLDAP** basieren.

Microsoft Active Directory ist der Verzeichnisdienst speziell für Microsoft Windows NT/2000-Netzwerke und erlaubt die zentrale Organisation und Verwaltung aller Netzwerkressourcen. Er ermöglicht den Benutzern über eine einzige zentrale Anmeldung den Zugriff auf alle Ressourcen und dem Administrator die zentral organisierte Verwaltung, transparent von der Netzwerktopologie und den eingesetzten Netzwerkprotokollen.
Für diesen Verzeichnisdienst wird zur Bewertung der Anfragen ein MS Windows NT/2000 Domain Controller benötigt.

Novell eDirectory – Novell Directory Service 8 - ist ein auf X.500 basierender Verzeichnisdienst zur Verwaltung von Benutzern, Zugriffsrechten und anderen Netzwerkressourcen. Novell stellt den Verzeichnisdienst für die Plattformen Netware ab Version 5, MS Windows NT/2000, Linux und Solaris zur Verfügung.

Mit Hilfe des Open-Source-Projekts **OpenLDAP**, das unter der Aufsicht der **OpenLDAP Foundation** realisiert wird, kann in einem Netzwerk ein Verzeichnisdienst mit unterschiedlichen Stand-alone-LDAP-

Servern aufgebaut werden. Auf der Open-Source-Software basiert z. B. der Stand-alone-LDAP-Server **iPlanet Directory Server**.

Benutzerauthentifizierung

Bei der Benutzerauthentifizierung über **LDAP** wird im Verzeichnisdienst der **Distinguished Name (DN)** des Benutzers abgefragt. Der abgefragte Name des Benutzers muss innerhalb des Verzeichnisses einmalig sein.

Bei **Microsoft Active Directory (AD)** und **Novell eDirectory (NDS8)** hat jedes Objekt einen definierten **DN**, der die Domain und den Pfad im AD-Verzeichnis, bzw. im NDS-Baum identifiziert und in der Gesamtstruktur eindeutig ist. Dieser **DN** setzt sich aus **Common Name (CN)** und **Domain Component (DC)** zusammen.
Beispiel: CN=Administrator, CN=Users, DC=example, DC=com

Unter **MS Active Directory** kann die Benutzerauthentifizierung auch durch den **User Principal Name (UPN)** erfolgen. Dieser Name besteht aus dem Anmeldenamen und dem DNS-Namen der Domain.
Beispiel: admin@example.com

Unter **OpenLDAP** erfolgt eine einfache Abfrage nach dem **Common Name (CN)**. Hierbei ist zu beachten, dass jedem eingetragenen Benutzer ein eindeutiger **CN** zugeordnet sein muss.



Sicherheitshinweis:

Bei der Benutzerauthentifizierung mittels Stand-alone-LDAP-Server werden ausschließlich Klartextpasswörter verwendet. Ohne die *TLS-Verschlüsselung* (*TLS encryption*) ist es somit in ungeswitchten Umgebungen möglich, Passwörter, die vom Sicherheitssystem gesendet werden mitzulesen.

Hinweis:

Für die Benutzerauthentifizerung mittels **LDAP-Server** muss im Menü **Proxies/DNS** der **DNS-Proxy** eingeschaltet und konfiguriert sein.

Microsoft Active Directory-Server einstellen:

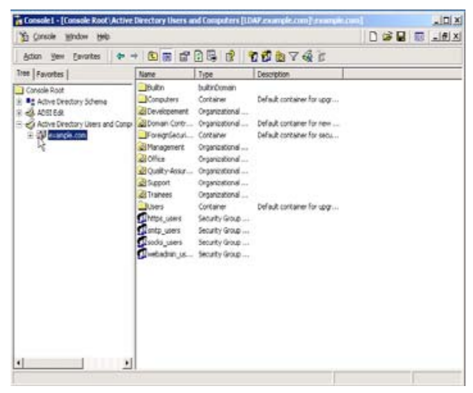
Auf dem Stand-alone-LDAP-Server muss ein Benutzer eingerichtet sein, der die Leserechte für das gesamte Verzeichnis hat.



Sicherheitshinweis:

Stellen Sie sicher, dass dieser Benutzer **nur** die Leserechte bekommt.

Bei **Microsoft Active Directory (AD)** sollte der Abfrage-Typ **MemberOf** verwendet werden, da sich ein bereits vollständig eingerichteter Verzeichnisdienst einfach erweitern lässt.
Das Verzeichnis (Directory) kann wiederum um selbstdefinierte Attribute erweitert werden. Diese Attribute, die für jeden Benutzer einzeln auf dem Directory-Server gesetzt werden müssen, geben durch den Wert oder den Inhalt Auskunft welche Berechtigungen dem Benutzer zugewiesen wurden.



In diesem Konfigurations-Beispiel wird die kleine Domain **example.com** dargestellt:

Im Verzeichnis **Trainees** befindet sich der Benutzer **Hans Mustermann**.
DN: cn=hans mustermann, ou=trainees, dc=example, dc=com.
LogonName: mustermann@example.com

Dieser Benutzer könnte sich mit seinem LogonName und seinem Passwort z. B. am SOCKS-Proxy anmelden. Das Internet-Sicherheitssystem überprüft in diesem Fall den DN und das Passwort von Hans Mustermann. Falls es dann zum LogonName mustermann@example.com einen eindeutigen DN gibt, und das eingegebene Passwort gültig ist, kann der Benutzer den Dienst SOCKS verwenden.

Falls Sie den Abfrage-Typ **MemberOf** verwenden möchten führen Sie am Stand-alone-LDAP-Server **Microsoft Active Directory** folgende Einstellungen durch:

Schritt 1 - Erstellen einer Security Group:

1. Klicken Sie in der **Microsoft Management Console** mit der rechten Maustaste auf die Domain.

   Beispiel: Domain **example.com**

2. Klicken Sie mit der linken Maustaste auf die Schaltfläche **New** und anschließend auf **Group**.

   Anschließend öffnet sich das Fenster **New Object - Group**.

3. Definieren Sie im Eingabefeld **Group name** einen eindeutigen Namen für die Gruppe.

   Beispiel: **socks_users** für den SOCKS-Proxy

1. Wählen Sie bei **Group type** die Option **Security** aus.

2. Speichern Sie die Eingaben durch einen Klick auf die Schaltfläche **OK**.

   Sie haben nun die neue **Security Group** mit dem Namen **socks_users** erstellt.

Schritt 2 - Benutzer der Security Group zuweisen:

1. Wählen Sie im Verzeichnis den Benutzer aus und klicken mit der rechten Maustaste auf den Namen.

   Beispiel: **Hans Mustermann** im Verzeichnis **Trainees**.

2. Klicken Sie mit der linken Maustaste auf die Schaltfläche **Properties**.

   Anschließend öffnet sich das Fenster **Properties**.

3. Wählen Sie im Fenster **Properties** das Register **MemberOf** aus.

4. Um die neue Gruppe auszuwählen, klicken Sie auf die Schaltfläche **Add**.

   Anschließend öffnet sich das Fenster **Select Groups**.

5. Wählen Sie nun die **Security Group** aus.

   Beispiel: **socks_users**

6. Speichern Sie die Eingabe durch einen Klick auf die Schaltfläche **OK**.

   Die neue **Security Group** wurde nun in das Fenster **MemberOf** übernommen.

7. Speichern Sie die Eingaben durch einen Klick auf die Schaltfläche **OK**.

Führen Sie nun die Einstellungen auf dem Internet-Sicherheitssystem durch. Die Einstellungen am Konfigurationstool **WebAdmin** werden ab Seite 112 erklärt.

Microsoft Active Directory, selbstdefinierte Attribute:

Die Benutzerauthentifizierung mittels Microsoft Active Directory kann auch mit zusätzlich selbstdefinierten Attributen und Werten erfolgen. Die Konfiguration ist allerdings sehr viel aufwendiger.

Hinweis:

Um eine derartige Erweiterung unter MS Active Directory durchzuführen, benötigen Sie für jedes Attribut eine **Objekt ID (OID)**. Die OID-Nummer ist im gesamten Internet einzigartig und wird an Unternehmen von der **Internet Assigned Numbers Authority (IANA)** ausgestellt. Die OID der Astaro AG ist z. B. 1.3.6.1.4.1.9789.

Falls Sie noch keine OID-Nummer haben, können Sie diese direkt bei der **IANA** unter der Internetadresse **www.iana.org** beantragen. Überlegen Sie im ersten Schritt, wie Sie diese OID-Nummer am besten Ihrer Netzwerkstruktur anpassen und erweitern. Beachten Sie, dass für jedes Benutzerattribut eine eigene OID benötigt wird.

Für die Erstellung weiterer Attribute muss die **Microsoft Management Console** zuvor um das **Active Directory Schema** ergänzt werden. Des Weiteren müssen Sie gewährleisten, dass Sie dieses Schema bearbeiten bzw. erweitern und verändern dürfen.

Schritt 1 – Active Directory Schema freigeben:

1. Klicken Sie in der **Microsoft Management Console** mit der rechten Maustaste auf **Active Directory Schema**.

2. Klicken Sie mit der linken Maustaste auf die Schaltfläche **Operations Master**.

   Anschließend öffnet sich das Fenster **Change Schema Master**.

3. Markieren Sie das Optionsfeld **The Schema may be modified on this Domain Controller**.

4. Speichern Sie die Eingabe durch einen Klick auf die Schaltfläche **OK**.

Sie sind nun berechtigt, das **Active Directory Schema** zu bearbeiten.

Schritt 2 – Neues Attribute erstellen:

1. Klicken Sie mit der rechten Maustaste unter **Active Directory Schema** auf das Verzeichnis **Attribute**.
2. Klicken Sie mit der linken Maustaste auf die Schaltfläche **New**.
3. Definieren Sie im Fenster **Create New Attribute** das neue Attribut.

   Common Name: Tragen Sie in das Eingabefeld den **CN** ein.

   LDAP Display Name: Vergeben Sie für das neue Attribut einen eindeutigen Namen. Am Besten denselben Namen, den Sie für diesen Dienst (Service) auch auf dem Internet-Sicherheitssystem verwendet haben.
   Beispiel: **Socks**.

   Unique X500 Object ID: Tragen Sie in das Eingabefeld die OID-Nummer ein.

   Syntax: Wählen Sie **Boolean** aus.

   Minimum: Lassen Sie dieses Eingabefeld leer.

   Maximum: Lassen Sie dieses Eingabefeld leer.
4. Speichern Sie die Eingaben durch einen Klick auf die Schaltfläche **OK**.

Schritt 3 – Attribut einer Klasse (Class) zuweisen:

1. Klicken Sie mit der linken Maustaste unter **Active Directory Schema** auf das Verzeichnis **Classes**.
2. Klicken Sie mit der rechten Maustaste auf das Verzeichnis **Users**.

   Anschließend öffnet sich das Fenster **User Properties**.

3. Klicken Sie auf das Register **Attributes** und führen Sie die folgenden Einstellungen durch.

   Optional: Wählen Sie im Auswahlfeld das Attribut aus und übernehmen Sie dieses durch einen Klick auf die Schaltfläche **Add**.
   Beispiel: **Socks**.

4. Speichern Sie die Eingaben durch einen Klick auf die Schaltfläche **OK**.

5. Klicken Sie in der **Microsoft Management Console** mit der rechten Maustaste auf **Active Directory Schema**.

6. Klicken Sie mit der linken Maustaste auf die Schaltfläche **Reload the Schema**.

Schritt 4 – Attribut einem Benutzer (User) zuweisen:

1. Klicken Sie im Verzeichnis **ADSI Edit** mit der rechten Maustaste auf den entsprechenden Benutzer.

   Beispiel: **Hans Mustermann** im Verzeichnis **Trainees**.

2. Klicken Sie mit der linken Maustaste auf die Schaltfläche **Properties**.

   Anschließend öffnet sich das Fenster **Properties**.

3. Wählen Sie im Fenster **Properties** das Register **Attributes** aus und führen Sie die folgenden Einstellungen durch.

   Select which properties to view: Wählen Sie **Both** aus.

   Select a property to view: Wählen Sie hier das Attribut aus.
   Beispiel: **Socks**.

   Syntax: Dieser Wert wird beim Erstellen des Attributs gesetzt und kann hier nicht mehr geändert werden.
   Beispiel lt. Schritt 2: **Boolean**.

   Edit Attribut: Mit diesem Eingabefeld kann der Wert des Attributs editiert werden. Mögliche Werte sind **TRUE** oder **FALSE**.

Value(s): Hier wird der Wert des Attributs angezeigt.

4. Speichern Sie die Eingaben durch einen Klick auf die Schaltfläche **OK**.

Führen Sie nun die Einstellungen auf dem Internet-Sicherheitssystem durch. Die Einstellungen am Konfigurationstool **WebAdmin** werden ab Seite 112 erklärt.

Novell-eDirectory-Server einstellen:

Auf dem Stand-alone-LDAP-Server muss ein Benutzer eingerichtet sein, der die Leserechte für das gesamte Verzeichnis hat.



Sicherheitshinweis:

Stellen Sie sicher, dass dieser Benutzer **nur** die Leserechte bekommt.

Bei **Novell eDirectory (NDS8)** sollte der Abfrage-Typ **groupMembership** verwendet werden, da sich ein bereits vollständig eingerichteter Verzeichnisdienst einfach erweitern lässt.
Das Verzeichnis kann wiederum um selbstdefinierte Attribute erweitert werden. Diese Attribute, die für jeden Benutzer einzeln auf dem Directory-Server gesetzt werden müssen, geben durch den Wert oder den Inhalt Auskunft welche Berechtigungen dem Benutzer zugewiesen wurden.
Für die Konfiguration des Novell eDirectory-Servers benötigen Sie die **Novell ConsoleOne**.

Die Verwaltung des Novell-eDirectory-Servers wird ausführlich in der zugehörigen Dokumentation beschrieben. Sie erhalten die Dokumentation unter der Internetadresse:

http://www.novell.com/documentation/lg/edir87/index.html

Führen Sie anschließend die Einstellungen am Internet-Sicherheitssystem durch. Die Einstellungen am Konfigurationstool **WebAdmin** werden ab Seite 112 erklärt.

OpenLDAP-Server konfigurieren:

Auf dem Stand-alone-LDAP-Server muss ein Benutzer eingerichtet sein, der die Leserechte für das gesamte Verzeichnis hat.



Sicherheitshinweis:

Stellen Sie sicher, dass dieser Benutzer **nur** die Leserechte bekommt.

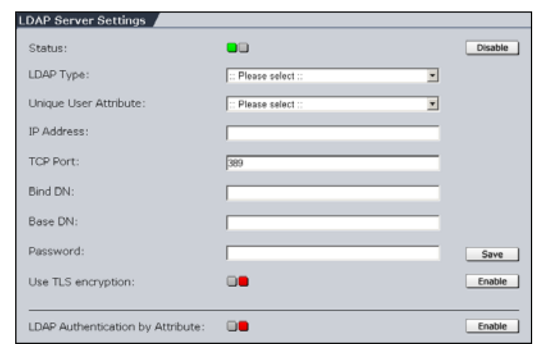
Unter **OpenLDAP** erfolgt zur Benutzerauthentifizierung eine einfache Abfrage nach dem **Common Name (CN)**. Hierbei ist zu beachten, dass jedem eingetragenen Benutzer ein eindeutiger **CN** zugeordnet sein muss.

Wichtiger Hinweis:

Bei der Installation der Software werden alle bestehenden Daten auf dem Rechner gelöscht!

Da es verschiedene Stand-alone-LDAP-Server gibt, die auf dem Open-Source-Projekt **OpenLDAP** basieren, entnehmen Sie die Informationen zur Installation und Konfiguration dieser Verzeichnisse der entsprechenden Dokumentation.
Falls Sie den Stand-alone-LDAP-Server **SLAPD** der **OpenLDAP Foundation** verwenden, erhalten Sie die aktuelle Dokumentation unter der Internetadresse: **http//www.openldap.org**.

LDAP auf Internet-Sicherheitssystem einstellen:



Auf dem Stand-alone-LDAP-Server muss ein Benutzer eingerichtet sein, der die Leserechte für das gesamte Verzeichnis hat.

Um die nötigen Einstellungen auf dem Internet-Sicherheitssystem durchzuführen, benötigen Sie den **Distinguished Name (DN)** dieses Benutzers sowie den LDAP-Type und die IP-Adresse des Stand-alone-LDAP-Servers.



Sicherheitshinweis:

Stellen Sie sicher, dass der Benutzer **nur** die Leserechte für den Stand-alone-LDAP-Server bekommt.

1. Öffnen Sie im Verzeichnis **System** das Menü **User Authentication**.

2. Schalten Sie die Funktion im Fenster **LDAP Server Settings** durch einen Klick auf die Schaltfläche **Enable** bei **Status** ein.

   LDAP Type: Wählen Sie in diesem Drop-down-Menü den Type des Stand-alone-LDAP-Servers aus.
   Die möglichen Typen sind: **Microsoft Active Directory**, **Novell eDirectory** und **OpenLDAP**.

   Unique User Attribute: Dieses Atribut definiert den Benutzernamen zur Authentifizierung am Stand-alone-LDAP-Server. Die zur Verfügung stehenden Atribute hängen vom ausgewählten Type des Stand-alone-LDAP-Servers ab. Falls Sie für den Benutzernamen ein eigenes Attribut erstellen möchten, wählen Sie hier **Selfdefined** aus (siehe nachfolgendes Bild).

Für den LDAP-Server **Microsoft Active Directory** können Sie das Atribut **User Principal Name (UPN)** oder **saMAccount-Name** auswählen.

Für die LDAP-Server **Novell eDirectory** und **OpenLDAP** kann jeweils das Attribut **Common Name (CN)**, **Surname (SN)** oder **Unique Identifier (UID)** eingestellt werden.



Attribute Name: Dieses Eingabefeld wird nur angezeigt, wenn im Drop-down-Menü **Unique User Attribute** die Einstellung **Selfdefined** ausgewählt wurde.

Definieren Sie in diesem Eingabefeld das eigene Attribut zur Bestimmung des Benutzernamens.

IP Address: Tragen Sie in das Eingabefeld die IP-Adresse des Stand-alone-LDAP-Servers ein.

TCP Port: Tragen Sie in das Eingabefeld den TCP Port ein. Per Default ist der Standard-Port 389 bereits eingetragen.

Bind DN: Der hier einzutragende Wert hängt vom Type des Stand-alone-LDAP-Servers ab:

1. Microsoft Active Directory

Sie können den **User Principal Name (UPN)** oder den gesamte **Distinguished Name (DN)** des Benutzers eintragen.

Beispiele:

UPN: admin@example.com

DN: cn=administrator, cn=users, dc=example, dc=com

2. Novell eDirectory

Tragen Sie in das Eingabefeld den gesamten **Distinguished Name (DN)** des Benutzers ein.

Beispiel:

DN: cn=administrator, o=our_organisation

3. OpenLDAP

Bei **OpenLDAP** oder OpenLDAP-konformen Stand-alone-Servern, kann nur der **Distinguished Name (DN)** des Benutzers eingetragen werden.

Base DN: Tragen Sie in das Eingabefeld die Objektnamen ein, von wo aus der Client den Vorgang startet.
Beispiele:
Für MS Active Directory: dc=example, dc=com
Für Novel eDirectory: o=our_organisation

3. Tragen Sie im Eingabefeld **Password** das Passwort ein. Dieses Passwort sollte auch für die Administration des Stand-alone-LDAP-Servers verwendet werden.



Sicherheitshinweis:

Setzen Sie sichere Passwörter! Ihr Vorname rückwärts buchstabiert ist beispielsweise kein ausreichend sicheres Passwort – besser wäre z. B. xfT35!4z.

4. Falls Sie die Verbindung zum LDAP-Server mit dem SSL/TLS-Standard verschlüsseln möchten, schalten Sie die Funktion in der Zeile **Use TLS encryption** durch einen Klick auf die Schaltfläche **Enable** ein.

   Durch die Verschlüsselung haben Sie die Möglichkeit die LDAP-Authentisierung auch über öffentliche Netzwerke zu nutzen.

5. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.



Sicherheitshinweis:

Solange die Funktion **LDAP Authentication by Attribute** ausgeschaltet ist, können alle Benutzer, die im Verzeichnisdienst einen eindeutigen **DN** und ein gültiges Passwort haben die Proxies **HTTP**, **SMTP** und **SOCKS** verwenden sowie auf das Konfigurationstool **WebAdmin** zugreifen.

LDAP, erweiterte Authentifizierung:

1. Schalten Sie die Funktion **LDAP Authentication by Attribute** durch einem Klick auf die Schaltfläche **Enable** bei **Status** ein.

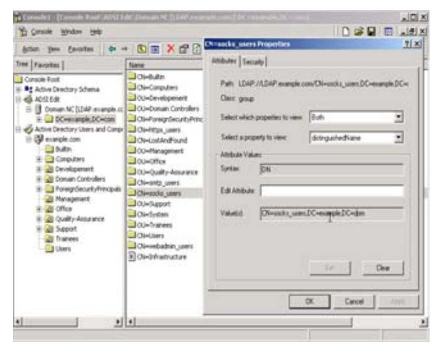
2. Wählen Sie im Drop-down-Menü **Service** den Dienst aus.

   Die möglichen Dienste sind: **HTTP**, **SMTP**, **SOCKS** und **Web-Admin**.

3. Tragen Sie in das Eingabefeld **Attribute Name** den Attributnamen ein.

   Falls Sie einen **Microsoft Active Directory**-Server verwenden und den Abfrage-Typ **MemberOf** konfiguriert haben, ist dies der Name der entsprechenden **Security Group**.
   Beispiel: **socks_users**.

4. Tragen Sie in das Eingabefeld **Attribute Value** den Attributwert ein. Der Attributwert ist der **DN**.



Bei **Microsoft Active Directory** wird der **DN** des Attributs über die **Management Console** im Verzeichnis **ADSI Edit** angezeigt:

Wählen Sie über den **Base DN** (Beispiel: dc=example, dc=com) den Attributnamen (Beispiel: socks _users) aus und klicken darauf mit der rechten Maustaste. Das Fenster **CN=socks_users Properties** wird geöffnet.
Wählen Sie nun im Drop-down-Menü **Select which properties to view** den Wert **Both** und im Drop-down-Menü **Select a property to view** den Wert **distinguishedName** aus. Der im Feld **Value(s)** angezeigte Wert ist der Attributwert.

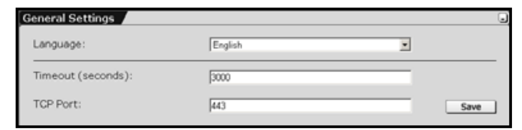
5. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

Nun ist jeder Benutzer, der als **MemberOf** der Security Group **socks _users** definiert wurde berechtigt diesen Dienst zu verwenden.

5.1.9. WebAdmin Settings

In diesem Menü richten Sie den Zugang zum Konfigurationstool **WebAdmin** ein.

General Settings



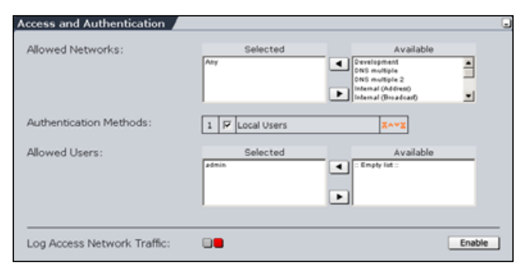
Language: In diesem Drop-down-Menü stellen Sie die Sprache ein.

Timeout (seconds): Im Eingabefeld geben Sie die Zeitspanne in Sekunden an, in der Sie vom **WebAdmin** automatisch abgemeldet werden, wenn keine Aktionen stattfinden. Nach der Installation sind standardmäßig 300 Sekunden eingestellt. Die kleinstmögliche Zeitspanne beträgt 60 Sekunden.
Speichern Sie die Eingabe durch einen Klick auf die Schaltfläche **Save**.

Wenn sie den Browser mit einer offenen **WebAdmin**-Session schließen ohne den **WebAdmin** über **Exit** zu verlassen, bleibt die letzte Session bis zum Ablauf des Time-outs aktiv.

TCP Port: Falls Sie den Standard-Port 443 für den HTTPS-Dienst anderweitig verwenden wollen (z. B. eine Umleitung mit **DNAT**), müssen Sie hier einen anderen TCP Port für das **WebAdmin** Interface angeben. Mögliche Werte sind 1024-65535, wobei bestimmte Ports für andere Dienste reserviert sind. Um den **WebAdmin** nach einer Änderung anzusprechen, müssen Sie den Port mit einem Doppelpunkt getrennt an die Sicherheitssystem-IP-Adresse anhängen,
z. B.: https://192.168.0.1 :1443.

Access and Authentication



Allowed Networks: Im Auswahlfeld werden die Netzwerke hinzugefügt, von denen aus auf **WebAdmin** zugegriffen werden darf. Wie auch bei **SSH** ist hier für eine reibungslose Installation **Any** eingetragen. In diesem Fall darf, falls das Passwort zur Verfügung steht, von überall auf **WebAdmin** zugegriffen werden.

Sicherheitshinweis:

Sobald Sie einschränken können, von wo aus das Internet-Sicherheitssystem administriert werden soll (z. B. Ihre IP-Adresse im lokalen Netzwerk), ersetzen Sie den Eintrag **Any** im Auswahlfeld **Allowed Networks** durch ein kleineres Netzwerk.

Am sichersten ist es, wenn nur ein Administrations-PC per HTTPS auf das Internet-Sicherheitssystem Zugriff hat.
Netzwerke definieren Sie im Menü **Definitions/Networks**.

Authentication Methods: Mit dem Auswahlfeld bestimmen Sie die Methode zur Authentifizierung. Damit Sie nach der Installation über das Konfigurationstool **WebAdmin** Zugriff auf das Internet-Sicherheitssystem haben, wurde hier bereits während der Installation die Authentifizierungsmethode **Local Users** definiert und im Auswahlmenü **Allowed Users** der entsprechende **Benutzer (User)** angelegt.

Weitere mögliche Authentifizierungsmethoden sind **NT/2000/XP Server**, **RADIUS Database** und **LDAP Server**.

Allowed Users: Per Default ist hier der Benutzer **admin** einegstellt.

Die lokalen **Benutzer (Users)** werden im Menü **Definitions/Users** verwaltet.

Log Access Network Traffic: Alle Verbindungen zum Konfigurationstool **WebAdmin** werden in den **Packet Filter Logs** als **Accept**-Regel protokolliert. Die **Packet Filter Logs** befinden sich im Menü **Local Logs/Browse**. Per Default ist diese Funktion ausgeschaltet. Die Funktion wird durch einen Klick auf die Schaltfläche **Enable** eingeschaltet (Statusampel zeigt Grün).

Block Password Guessing



Mit dieser Funktion können die Versuche sich in das Konfigurationstool **Web-Admin** einzuloggen begrenzt werden. Nach einer bestimmten Anzahl an Versuchen, wird der Zugang von dieser IP-Adresse aus für eine bestimmte Zeitspanne verweigert.

Blockierschutz für Login-Versuche einstellen:

1. Stellen Sie im Drop-down-Menü **After failed Attempts** die maximale Anzahl der Versuche ein.

2. Tragen Sie in das Eingabefeld **Block IP for Period** die Zeitspanne für den Blockierschutz ein.

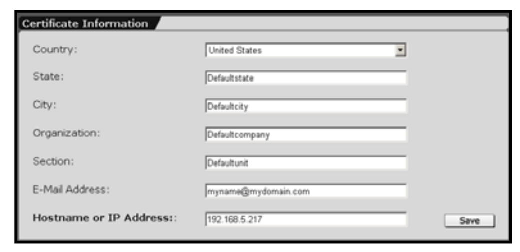
3. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

Der Blockierschutz ist nun eingestellt. Im Fenster **Never block Networks** können Sie Netzwerke oder Hosts vom Blockierschutz ausnehmen.

5.1.10. WebAdmin Site Certificate

Ein wichtiger Bestandteil des Sicherheitssystems sind die Verschlüsselungsverfahren. Diese kryptographischen Verfahren werden bei der Übertragung vertraulicher Daten über **Virtual Private Networks** (Kapitel 5.7 ab Seite 355), bei der **Benutzerauthentifizierung**, beim **Up2Date Service** sowie zur sicheren Administration des Internet-Sicherheitssystems angewendet.

Zertifikate und Certificate Authorities (CA) sind ein wesentlicher Bestandteil moderner kryptografischer Anwendungen und schließen die Sicherheitslücken, die bei anderen Algorithmen alleine noch offen bleiben. Eine sehr elegante Art verschlüsselt zu kommunizieren, sind die **Public-Key**-Algorithmen. Sie setzen jedoch voraus, dass die öffentlichen Schlüssel aller Partner bekannt sind.
Hier kommt eine vertrauenswürdige dritte Stelle ins Spiel, die für die Echtheit öffentlicher Schlüssel sorgt. Zu diesem Zweck stellt sie Zertifikate aus. Diese Stelle wird daher auch **Cerficate Authority (CA)** genannt. Ein Zertifikat ist ein Datensatz oder ein Text in einem standardisierten Format mit den wichtigsten Daten des Besitzers, seinem Namen und seinem öffentlichen Schlüssel, unterschrieben mit dem privaten Schlüssel der **CA**. Das Format der Zertifikate ist im X.509-Standard festgelegt.
In einem Zertifikat unterschreibt die **CA**, dass sie sich von der Echtheit einer Person überzeugt hat und dass der vorliegende öffentliche Schlüssel zu der Person gehört. Da das Zertifikat Werte wie den Namen des Besitzers, die Gültigkeitsdauer, die ausstellende Behörde und einen Stempel mit einer Unterschrift der Behörde enthält, kann es auch als digitaler Pass betrachtet werden.



Mit Hilfe dieses Menüs erzeugen Sie zwei Zertifikate: Zum einen das CA-Zertifikat, welches im Zertifikatspeicher Ihres Browsers installiert wird und zum anderen ein Server-Zertifikat, das wiederum das Internet-Sicherheitssystem benötigt, um sich bei Ihrem Browser zu authentifizieren. Diese zwei Zertifikate prüfen die Firmendaten und den Sicherheitssystem-Hostnamen.

Zertifikat für WebAdmin erstellen:

1. Öffnen Sie im Verzeichnis **System** das Menü **WebAdmin Site Certificate**.

2. Tragen Sie im Fenster **Certificate Information** die entsprechenden Firmendaten in das Drop-down-Menü und die Eingabefelder ein.

Country: Wählen Sie in diesem Drop-down-Menü das Land aus.

State: Tragen Sie das Bundesland ein.

City: Tragen Sie die Stadt ein.

Organization: Tragen Sie den Firmennamen ein.

Section: Tragen Sie die Abteilung ein.

E-Mail Address: Tragen Sie die E-Mail-Adresse ein, über die Sie eventuell kontaktiert werden möchten.

3. Tragen Sie in das Eingabefeld **Hostname or IP Address** den Hostnamen oder die IP-Adresse des Sicherheitssystems ein, über die Sie mit Ihrem Browser auf **WebAdmin** zugreifen.

Beispiel: Wenn Sie über die Adresse https://192.168.10.1 auf das Konfigurationstool **WebAdmin** zugreifen, tragen Sie 192.168.10.1 in das Eingabefeld ein.

4. Speichern Sie nun Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

Zertifikat für WebAdmin installieren:

1. Um nun das CA-Zertifikat auf Ihrem Browser zu installieren, klicken Sie im Fenster **Certificate Installation** auf die Schaltfläche **Install Certificate into Browser**.

   Die anschließenden Dialoge sind von Ihrem Browsertyp abhängig. Bei Microsoft Internet Explorer z. B. öffnet sich der Dialog **Dateidownload**:

   Datei auf Datenträger speichern: Mit dieser Option können Sie das Zertifikat vor der Installation auf einem lokalen Datenspeicher sichern.

   Die Datei von ihrem aktuellen Ort öffnen: Mit dieser Option wird das Zertifikat direkt geöffnet. Im Fenster **Zertifikat** haben Sie anschließend drei Register zur Verfügung. In diesen Registern können Sie die Daten Ihres Zertifikats betrachten und anschließend installieren.

2. Um den jeweiligen Vorgang zu starten, klicken Sie auf die Schaltfläche **OK**.

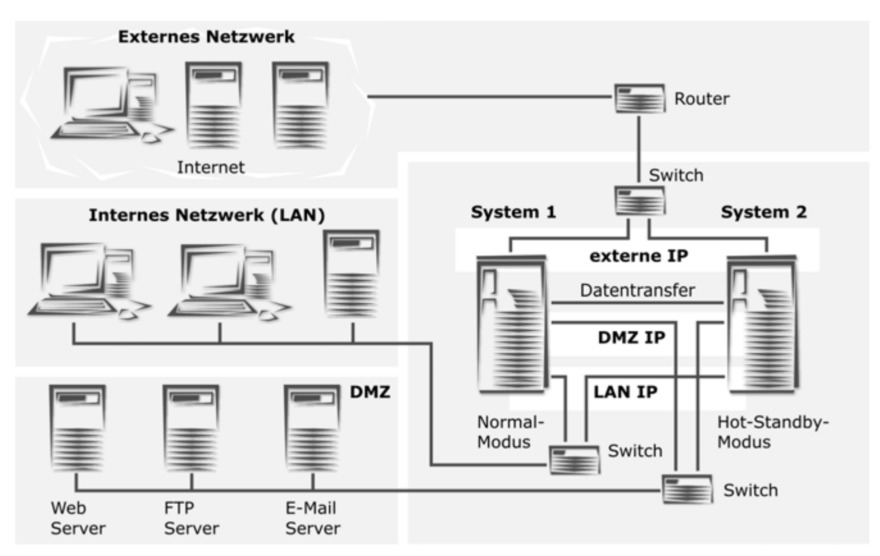
Hinweis:

Infolge von unterschiedlichen Systemzeiten und den weltweit versetzten Zeitzonen, kann es vorkommen, dass das Zertifikat nicht sofort gültig ist. Viele Browser versenden dann die Meldung, dass das Zertifikat abgelaufen sei. Diese Meldung ist nicht richtig. Das neu generierte Zertifikat wird nach maximal 12 Stunden gültig.

5.1.11. High Availability

Der häufigste Grund für den Ausfall eines Internet-Sicherheitssystems, bzw. einer Firewall ist ein Defekt der Hardware, z. B. des Netzteils, der Festplatte oder des Prozessors. Bei diesem **High-Availability-(HA)**-System werden zwei Sicherheitssysteme mit identischer Hardware parallel geschaltet. Das Sicherheitssystem 1 läuft im Normal-Modus (Master). Das Sicherheitssystem 2 befindet sich im Hot-Standby-Modus (Slave) und überwacht das aktive System über die Datentransfer-Leitung mittels Link Beat. Das Sicherheitssystem 1 schickt über diese Verbindung in regelmäßigen Abständen Heart-Beat-Anfragen, die vom System 2 beantwortet werden. Über die Datentransfer-Leitung wird das Sicherheitssystem 2 bei Bedarf auch aktualisiert, damit es bei einem Ausfall des aktiven Systems sofort deren Funktion übernehmen kann.

In der Grafik ist eine Netzwerkarchitektur mit einem *High-Availability-(HA)*-System dargestellt, an die ein internes Netzwerk und eine DMZ angeschlossen sind. In der Installationsanleitung wird beschrieben, wie ein privates Netzwerk an das *HA*-System angeschlossen wird:



Hardware- und Software-Voraussetzungen

- Eine Lizenz mit der Option **High Availability**: Die **Lizenzdatei** (**License Key**) muss auf beiden Sicherheitssystemen (Normal- und Hot-Standby-Modus) eingespielt werden!

  Weitere Informationen zur **Lizenzierung** erhalten Sie in Kapitel 5.1.2 ab Seite 56.
- Zwei Sicherheitssysteme mit identischer Software-Version und identischer Hardware
- Zwei zusätzliche Ethernet-Netzwerkkarten für die Datentransfer-Leitung: Für die Überwachung mittels Heart-Beat-Anfragen werden zwei Ethernet-Netzwerkkarten benötigt, die diese Funktion unterstützen!
- Ein Ethernet-Crossover-Kabel
- Ein serielles Schnittstellenkabel (optional)
- Zwei Switches

Wichtiger Hinweis:

Für die Überwachung mittels Heart-Beat-Anfragen werden zwei Ethernet-Netzwerkkarten benötigt, die vom Sicherheitssystem unterstützten werden. Die **Hardware Compatibility List (HCL)** befindet sich auf **http://www.astaro.com/kb**. Mit Hilfe des Suchbegriffs **HCL** gelangen Sie schnell auf die entsprechende Seite.

Wichtiger Hinweis:

Falls Sie für das **High-Availability-(HA)**-System ein bereits im Einsatz befindliches Sicherheitssystem verwenden, achten Sie darauf, dass Sie das zweite Sicherheitssystem vor Beginn der Konfiguration auf die selbe Version wie System 1 updaten.

High Availability-System installieren

In dieser Installationsanweisung werden die erforderlichen Einstellungen beschrieben, wenn das **High-Availability**-System an ein internes Netzwerk angeschlossen wird. Für dieses Szenarium benötigen Sie auf beiden Sicherheitssystem drei Netzwerkkarten: Eine zum *internen Netzwerk* (eth0), eine zum *Internet* (eth1) und eine für die *Datentransfer-Leitung* (eth2) zwischen den beiden Sicherheitssystemen. Für jedes weitere interne Netzwerk (z. B. ein DMZ) wird ein weiteres Switch benötigt.

Vorbereitung:

1. ***Software auf beiden Rechnern installieren:***

Installieren Sie die Software auf den beiden Rechnern.

Die Installation der Software wird in Kapitel 3.2.1 ab Seite 25 beschrieben.

2. ***Konfigurationstool WebAdmin starten und System-Passwörter setzen:***

Setzen Sie auf beiden Sicherheitssystem alle erforderlichen Passwörter. Falls das **High-Availability**-System später mit dem **Astaro Configuration Manager** konfiguriert und verwaltet wird, müssen Sie auch das Passwort **Astaro Configuration Manager user** (**wwwrun**) setzen.

3. ***Hardware miteinander verbinden:***

Um die Hardware-Komponenten (System 1 und 2, Switches etc.) wie auf der Grafik dargestellt miteinander zu verbinden, müssen Sie wissen, welcher Netzwerkkarte welche **Sys ID** auf dem jeweiligen Sicherheitssystem zugewiesen wurde.

Die Schnittstellen müssen auf beiden Sicherheitssystemen identisch konfiguriert werden. Netzwerkkarten mit der gleichen **Sys ID** müssen an dasselbe Netzwerk angeschlossen werden: Die

Schnittstelle mit der **Sys ID eth2** wird hier z. B. für die Datentransfer-Leitung verwendet.

Um die Zuordnung der **Sys ID** zu ermitteln, öffnen Sie im Konfigurationstool **WebAdmin** das Menü **Network/Interfaces**.

In der Tabelle **Hardware Device Overview** sind alle auf dem Sicherheitssystem installierten Netzwerkkarten aufgelistet.

Falls es sich bei den Netzwerkkarten um Hardware verschiedener Hersteller und/oder Typs handelt, können Sie hier die Zuordnung der **Sys ID** ablesen und auf der Hardware entsprechend kennzeichnen. Wenn es sich um gleiche Netzwerkkarten handelt, gehen Sie folgendermaßen vor:

Während der Installation der Software wurde bereits die interne Netzwerkkarte (eth0) konfiguriert. Um nun bei den anderen Netzwerkkarten die **Sys ID** zuzuordnen, richten Sie mit Ausnahme der *Schnittstelle für die Datentransfer-Leitung* (z. B. die **Sys ID eth2**) alle Netzwerkkarten als **Standard-Ethernet**-Netzwerkkarten ein.

Wichtiger Hinweis:

Die Netzwerkkarte für die Datentransfer-Leitung darf im Menü **Network/Interfaces** nicht konfiguriert werden. Diese Schnittstelle wird später im Menü **System/High Availability** eingerichtet. Für die Überwachung mittels Heart-Beat-Anfrage reservieren Sie eine Netzwerkkarte, die diese Funktion unterstützt.

Verbinden Sie nun nacheinander Ihren Client mit den Netzwerkkarten des Sicherheitssystems und führen den Ping-Befehl aus. Anhand der entprechenden IP-Adresse können Sie dann die jeweilige **Sys ID** zuordnen.

Fahren Sie anschließend beide Sicherheitssysteme herunter und verbinden Sie die Hardware-Komponenten miteinander, wie in der Grafik auf Seite 122 dargestellt.

4. *Sicherheitssystem 1 (Normal-Modus) konfigurieren:*

Öffnen Sie im Verzeichnis **System** das Menü **High Availability**.

Schalten Sie die Option durch einem Klick auf die Schaltfläche **Enable** bei **Status** ein.

Device Name: Tragen Sie in das Eingabefeld einen eindeutigen Gerätenamen ein. Dieser Namen dient Ihnen zur Orientierung, welches der beiden Systeme zur Zeit im Normal-Modus läuft. Der Gerätenamen kann maximal 11 Zeichen lang sein.

Encryption Key: Tragen Sie in das Eingabefeld ein Passwort ein.



Sicherheitshinweis:

Setzen Sie sichere Passwörter! Ihr Vorname rückwärts buchstabiert ist beispielsweise kein ausreichend sicheres Passwort – besser wäre z. B. xfT35!4z.

Network Interface Card: Wählen Sie für die Datentransfer-Verbindung eine Netzwerkkarte (Beispiel: **eth2**) aus. Zur Auswahl stehen nur Netzwerkkarten, die zuvor im Menü **Network/ Interfaces** noch nicht konfiguriert wurden.

Wichtiger Hinweis:

Die Netzwerkkarten müssen auf beiden Systemen die gleiche **Sys ID** haben (z. B. eth 2). Für die Überwachung mittels Heart-Beat-Anfrage wählen Sie in diesem Auswahlfeld bei beiden Systemen (Normal-Modus und Hot-Standby-Modus) eine Netzwerkkarte aus, die diese Funktion unterstützt.

Device IP: Weisen Sie jedem Sicherheitssystem innerhalb der HA-Gerätegruppe eine IP-Adresse aus einem Class-C-Netzwerk zu. Die IPs müssen in einem Adressbereich liegen und dürfen innerhalb dieser Gerätegruppe nur einmal verwendet werden. Beispiel: Das *Internet-Sicherheitssystem 1* erhält die *Device IP 10.0.14.1* und das *Sicherheitssystem 2* die *Device IP 10.0.14.2*.

Hinweis:

Für die Datentransfer-Verbindung kann nur ein Class-C-Netzwerk – Netzwerkmaske 255.255.255.0 - verwendet werden. Die Bit-Masken-Darstellung kann hier nicht eingegeben werden. Das für den Datenaustausch definierte Netzwerk darf nirgends sonst verwendet werden.

Serial Interface (optional): Zusätzlich zur Datentransfer-Verbindung kann die Überwachung des aktiven Systems durch das Hot-Standby-System über die serielle Schnittstelle erfolgen. Über diese Verbindung erfolgt kein Datenaustausch. Wählen Sie im Drop-down-Menü die entsprechende serielle Schnittstelle aus.

Hinweis:

Wenn Sie nun die Eingaben wie nachfolgend beschrieben speichern, wird das System im Anschluss heruntergefahren und sofort wieder gestartet.

Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

Das System 1 wird nun neu gebootet. Falls eine Tastatur angeschlossen ist, blinkt auf dem Keyboard die LED-Anzeige **Num Lock**.

Sobald das System den Hot-Standby-Modus erreicht, ertönen kurz hintereinander zwei Beeps und die LED-Anzeige hört auf zu blinken. Da das System 2 noch ausgeschaltet ist, bootet das System 1 weiter in den Normal-Modus und die LED-Anzeige **Num Lock** blinkt wieder.

Nachdem das System 1 den Bootvorgang abgeschlossen hat, hört die LED-Anzeige **Num Lock** auf zu blinken und es ertönen im Sekundentakt fünf Beeps: Die MiddleWare hat nun alle Services, Regeln und Prozesse geladen und initialisiert.

Hinweis:

Falls die Signaltöne nicht ertönen und die LED-Anzeige noch blinkt, konnte die MiddleWare nicht alle Dienste, Regeln und Prozesse initialisieren. Wenden Sie sich in diesem Fall an den Support Ihres Sicherheitssystem-Anbieters.

5. ***Sicherheitssystem 2 (Hot-Standby-Modus) konfigurieren:***

   Starten Sie das System 2 und führen Sie auch auf System 2 Schritt 4 durch und klicken Sie anschließend zur Bestätigung auf die Schaltfläche **Save**.

   Das System 2 wird nun neu gebootet. Falls eine Tastatur angeschlossen ist, blinkt auf dem Keyboard die LED-Anzeige **Num Lock**.

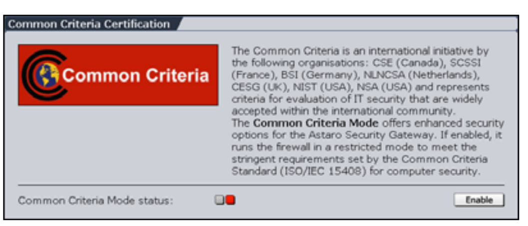
   Sobald das System den Hot-Standby-Modus erreicht, ertönen kurz hintereinander zwei Beeps und die LED-Anzeige hört auf zu blinken. Das System 2 erkennt über die Datentransfer-Leitung das aktive System 1 und verbleibt im Hot-Standby-Modus.

Das **High-Availability**-System ist nun aktiv.

Über die Datentransfer-Verbindung wird das Internet-Sichereitssystem im Hot-Standby-Modus ständig aktualisiert. Sobald das aktive System wegen einem Hardware-Defekt ausfällt, fährt das zweite System automatisch in den Normal-Modus und übernimmt dessen Funktion.

5.1.12. Certifications

Common Criteria Certification



In sensiblen Einsatzbereichen wie Banken, Versicherungen sowie im staatlichen und militärischen Sektor spielen Vertraulichkeit und Integrität von Hard- und Software schon immer eine große Rolle. Die Evaluierungsorganisationen haben daher ihren Ursprung in amtlichen Stellen, die für die Bewertung von militärischen und staatlichen Rechnersystemen zuständig waren. An der Definition der **Common Criteria for Information Technology Security Evaluation** sind neben den Europäischen Staaten Deutschland, Frankreich, den Niederlanden und Großbritanien auch Kanada und die USA beteiligt. Inzwischen liegt die Version 2.1 der Common Criteria vor, die als International Standard ISO/ IEC 15408 weltweit zur Beurteilung eines Produkts Gültigkeit hat.

Sie können das Sicherheitssystem so konfigurieren, dass sie der Definition der Common Criteria entspricht. Die Systemkonfiguration, die diesen Anforderungen entspricht wird als **Bewertete Konfiguration** (*Evaluated Configuration*) bezeichnet. Bei der Bewertung des Sicherheitssystems wurden allerdings nicht alle Sicherheitsfunktionen oder alle Methoden zur Erreichbarkeit der erforderlichen Stufe berücksichtigt. Diese Sicherheitsfunktionen und Methoden können von Ihnen trotzdem eingesetzt werden, allerdings läuft Ihre Firewall dann nicht mehr in der *Bewerteten Konfiguration*.

Hinweis:

Neben den Sicherheitsfunktionen, die in diesem Menü automatisch für die **Bewertete Konfiguration** eingeschaltet werden, müssen auch einige Einstellungen separat manuell durchgeführt werden. Die Richtlinien für eine vollständig konforme Konfiguration gemäß *Common Criteria* sind im **CC Guide** beschrieben.

Der *CC Guide* ist auf **http://www.astaro.com/kb** verfügbar. Die Zusatzdokumentation (*Guides*) zur **Astaro Security Gateway** Software finden Sie über die Navigation auf der linken Seite im Unterverzeichnis **Astaro Manuals and Guides**.

Um den **Common Criteria Mode** auf dem Sicherheitssystem zu starten klicken Sie auf die Schaltfläche **Enable**.

Schalten Sie anschließend im Menü **Packet Filter/Advanced** die folgenden Einstellungen ein:

- Strict TCP Session Handling
- Spoofing Protection (Einstellung *Strict*)
- Validate IP Packet Length

Hinweis:

Wenn Sie auf dem Sicherheitssystem im **Common Criteria Mode** eine der Funktionen manuell ausschalten, arbeitet das Sicherheitssystem nicht mehr mit der **Bewerteten Konfiguration**. Der *Common Criteria Mode* wird in diesem Fall automatisch deaktiviert.

ICSA Labs Certification



Die Firewall ist durch **ICSA Labs** gemäß ihren Anforderungen für Firewalls (Firewall Certification Criteria Version 4.0) zertifiziert. Solange die Firewall bei *Network Security Lab* entwickelt und die jeweils aktuelle Version in regelmäßigen Abständen stichprobenweise geprüft wird bleibt die Zertifizierung durch *ICSA Labs* erhalten.

Damit das Sicherheitssystem in einem *ICSA Labs* konformen Modus läuft, müssen die nachfolgend aufgeführten Funktionen eingeschaltet sein. Die folgenden Funktionen befinden sich im Menü **Packet Filter / Advanced**:

- Strict TCP Session Handling
- Spoofing Protection (Einstellung *Strict*)
- Validate IP Packet Length
- Log FTP Data Connections
- Log Unique DNS Requests

Die folgende Funktion befindet sich im Menü **Packet Filter / ICMP**:

- Log ICMP Redirects

Zusätzlich muss die folgende Funktion im Menü **Packet Filter / ICMP** ausgeschaltet sein:

- Firewall is Ping Visible

Um den **ICSA Labs Compliant Mode** der Firewall zu starten klicken Sie auf die Schaltfläche **Enable**.

5.1.13. Shut down/Restart

Mit **Restart** wird das Internet-Sicherheitssystem heruntergefahren und wieder gestartet. Der **Restart** kann je nach Hardware und Konfiguration bis zu 5 Minuten dauern.

Restart:

1. Öffnen Sie im Verzeichnis **System** das Menü **Shut down/ Restart**.
2. Wählen Sie im Drop-down-Menü **Action** die Aktion **Restart** aus.
3. Bestätigen Sie Ihre Auswahl durch einen Klick auf die Schaltfläche **Start**.
4. Beantworten Sie die Frage **Do you really want to restart?** durch einen Klick auf die Schaltfläche **OK**.

Mit **Shut down** können Sie das Internet-Sicherheitssystem herunterfahren.

Für Applikationen ohne Bildschirm und/oder LCD-Display ist besonders interessant, dass nach dem das System heruntergefahren wurde ein akustisches Signal ertönt: Endlos-Beep mit einer Sekunde Pause.

Der Vorgang dauert je nach Hardware und Konfiguration bis zu 5 Minuten. Erst nachdem Sie das System heruntergefahren haben, zu erkennen an der **Power down**-Ausgabe, dürfen Sie es ausschalten. Wenn das System, vor dem Ausschalten, nicht ordnungsgemäß heruntergefahren wurde, muss beim nächsten Startvorgang die Integrität des Filesystems überprüft werden – dies verzögert den Startvorgang. Im schlimmsten Fall können sogar Daten verloren gehen.
Wenn der Startvorgang erfolgreich war, ertönt ein akustisches Signal: Fünf Beeps in Folge.

Shut down:

1. Öffnen Sie im Verzeichnis **System** das Menü **Shut down/ Restart**.
2. Wählen Sie im Drop-down-Menü **Action** die Aktion **Shut down** aus.
3. Bestätigen Sie Ihre Auswahl durch einen Klick auf die Schaltfläche **Start**.
4. Beantworten Sie die Frage **Do you really want to shut down?** durch einen Klick auf die Schaltfläche **OK**.

5.2. Netzwerke und Dienste (Definitions)

Netzwerke und Dienste werden im Verzeichnis **Definitions** für alle weiteren Einstellungen, z. B. Paketfilter, VPN und Proxies zentral definiert. Dies hat den Vorteil, dass Sie später einfach mit den jeweiligen Bezeichnungen (**Name**) arbeiten können. Für eine weitere Vereinfachung sorgt die Möglichkeit, Netzwerke und Dienste zu gruppieren. Wenn Sie später diesen Gruppen bestimmte Einstellungen zuweisen, gelten diese für alle darin enthaltenen Netzwerke und Dienste. Gruppen können auch wieder in übergeordnete Gruppen zusammengefasst werden. Außerdem definieren Sie in diesem Verzeichnis die lokalen Benutzer für die Proxydienste.

5.2.1. Networks



Im Menü **Networks** werden die Hosts und Netzwerke sowie die Netzwerkgruppen definiert.

Die definierten Netzwerke und Gruppen werden in der Netzwerktabelle aufgelistet. Per Default befinden sich in der Tabelle neben den Definitionen für die interne Netzwerkkarte eth0 weitere statisch eingetragene Netzwerke. Diese statischen Netzwerke können von Ihnen nicht editiert oder gelöscht werden. Die Host und Netzwerke lassen sich zu Gruppen zusammenfassen. Diese Gruppen werden behandelt wie einzelne Hosts und Netzwerke und können wieder Teil einer übergeordneten Gruppe sein.

Auf den folgenden Seiten wird erläutert welche Netzwerktypen zur Verfügung stehen und wie sie definiert werden.

Die Netzwerktypen werden durch Symbole angezeigt:

Die Symbole

Icon	Spalte	Anzeige / Einstellung
	Netzwerktyp	Netzwerkkarte
	Netzwerktyp	Host/Server
	Netzwerktyp	Netzwerk
	Netzwerktyp	Netzwerkgruppe
	Netzwerktyp	DNS-Server
	Netzwerktyp	DNS-Server (Multiple RRs)
	Netzwerktyp	IPSec-Benutzergruppe

Host hinzufügen:

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Networks**.

2. Klicken Sie auf die Schaltfläche **New Definition**.

Anschließend wird das Eingabefenster geöffnet.

3. Führen Sie die folgenden Einstellungen durch:

Name: Tragen Sie in das Eingabefeld einen eindeutigen Namen für den Host ein.

> Diesen Namen verwenden Sie später, z. B. um Paketfilterregeln zu setzen. Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9, Minus- und Leerzeichen sowie Unterstrich. Maximal 39 Zeichen sind möglich.

Type: Wählen Sie im Drop-down-Menü **Host** aus.

Address: Tragen Sie in das Eingabefeld die IP-Adresse ein.

Comment: Über das Eingabefeld können Sie optional einen Kommentar für den Host hinzufügen.

4. Speichern Sie den Host durch einen Klick auf die Schaltfläche **Add Definition**.

Nach erfolgreicher Definition wird der neue **Host** in die Netzwerktabelle eingetragen. Sie finden diesen Host jetzt unter seinem Namen auch in verschiedenen anderen Menüs wieder. Diesen Host könnten Sie z. B. unter **System / Remote Syslog** als **Remote Syslog Server** definieren.

Netzwerk hinzufügen:

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Networks**.

2. Klicken Sie auf die Schaltfläche **New Definition**.

   Anschließend wird das Eingabefenster geöffnet.

3. Führen Sie die folgenden Einstellungen durch:

   Name: Tragen Sie in das Eingabefeld einen eindeutigen Namen für das Netzwerk ein.

   > Diesen Namen verwenden Sie später, z. B. um Paketfilterregeln zu setzen. Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9, Minus- und Leerzeichen sowie Unterstrich. Maximal 39 Zeichen sind möglich.

   Type: Wählen Sie im Drop-down-Menü **Network** aus.

   Address / Netmask: Tragen Sie in das Eingabefeld die IP-Adresse ein und wählen Sie im Drop-down-Menü die Netzwerkmaske aus.

   Comment: Über das Eingabefeld können Sie optional einen Kommentar für das Netzwerk hinzufügen.

4. Speichern Sie das Netzwerk durch einen Klick auf die Schaltfläche **Add Definition**.

WebAdmin prüft nun Ihre Eingaben auf semantische Gültigkeit.

Nach erfolgreicher Definition wird das neue **Netzwerk** in die Netzwerktabelle eingetragen. Sie finden dieses Netzwerk jetzt unter

seinem Namen auch in verschiedenen anderen Menüs wieder.
Für dieses Netzwerk können Sie z. B. unter **Proxies/HTTP** den Zugriff auf den HTTP-Proxy freischalten.

DNS-Server hinzufügen:

Domain Name System (**DNS**) ist eine verteilte Datenbank, die den Namensraum im Internet verwaltet. Mit *DNS* kann entweder der Namen in eine IP-Adresse (Forward Lookup) oder im umgekehrten Fall, die Adresse in einen Namen (Reverse Lookup) umgesetzt werden. Bei diesem Sicherheitssystem wird die erste Variante eingesetzt.

Der Typ **DNS Hostname** sollte ausschließlich in Verbindung mit DynDNS-Endpunkten verwendet werden. Das Sicherheitssystem löst die Definition gemäß dem Time-to-live-Wert (TTL) auf und aktualisiert diese anschließend mit der neuen IP-Adresse. Diese Netzwerk-Definition kann in allen Konfigurationen verwendet werden. Sie ist besonders für *IPSec-VPN*-Endpunkte und *SMTP Route Targets* nützlich.

Der Typ **DNS Hostname (multiple records)** sollte universell für alle anderen Adressauflösungen verwendet werden, wenn nicht feststeht, dass von diesem *DNS* nur eine IP-Adresse abgebildet wird.

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Networks**.

2. Klicken Sie auf die Schaltfläche **New Definition**.

Anschließend wird das Eingabefenster geöffnet.

3. Führen Sie die folgenden Einstellungen durch:

Name: Tragen Sie in das Eingabefeld einen eindeutigen Namen für den DNS-Server ein.

> Diesen Namen verwenden Sie später, z. B. um Paketfilterregeln zu setzen. Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9, Minus- und Leerzeichen sowie Unterstrich. Maximal 39 Zeichen sind möglich.

Type: Wählen Sie im Drop-down-Menü **DNS Hostname** aus.

Hostname: Tragen Sie in das Eingabefeld den Hostnamen ein.

Comment: Über das Eingabefeld können Sie optional einen Kommentar für den DNS-Server hinzufügen.

4. Speichern Sie den Host durch einen Klick auf die Schaltfläche **Add Definition**.

Nach erfolgreicher Definition wird der neue **DNS-Server** in die Netzwerktabelle eingetragen. Sie finden diesen Host jetzt unter seinem Namen auch in verschiedenen anderen Menüs wieder.

Netzwerkgruppe definieren:

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Networks**.
2. Klicken Sie auf die Schaltfläche **New Definition**.

   Anschließend wird das Eingabefenster geöffnet.
3. Führen Sie die folgenden Einstellungen durch:

   Name: Tragen Sie in das Eingabefeld einen eindeutigen Namen für die Netzwerkgruppe ein.

   > Diesen Namen verwenden Sie später, z. B. um Paketfilterregeln zu setzen. Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9, Minus- und Leerzeichen sowie Unterstrich. Maximal 39 Zeichen sind möglich.

   Type: Wählen Sie im Drop-down-Menü **Network Group** aus.

   Initial Members: Wählen Sie im Auswahlfeld die Netzwerke aus, indem Sie auf der Tastatur die **Strg**-Taste gedrückt halten und mit der Maus die Namen markieren.

   Comment: Über das Eingabefeld können Sie optional einen Kommentar für die Netzwerkgruppe hinzufügen.
4. Speichern Sie die Netzwerkgruppe durch einen Klick auf die Schaltfläche **Add Definition**.

Nach erfolgreicher Definition wird die neue **Netzwerkgruppe** in die Netzwerktabelle eingetragen. Sie finden diese Netzwerkgruppe jetzt

unter seinem Namen auch in verschiedenen anderen Menüs wieder.

IPSec-Benutzergruppe definieren:

Diese Definition enthält nur den **Distinguished Name** (**DN**). Er wird für ankommende IPSec-Verbindungen, die X.509-Zertifikate verwenden eingesetzt. Wenn der DN der Gruppe mit dem des Benutzers übereinstimmt, wird seine virtuelle IP-Adresse dynamisch bei der Gruppe hinzugefügt.

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Networks**.

2. Klicken Sie auf die Schaltfläche **New Definition**.

   Anschließend wird das Eingabefenster geöffnet.

3. Führen Sie die folgenden Einstellungen durch:

   Name: Tragen Sie in das Eingabefeld einen eindeutigen Namen für die IPSec-Benutzergruppe ein.

   > Diesen Namen verwenden Sie später, z. B. um Paketfilterregeln zu setzen. Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9, Minus- und Leerzeichen sowie Unterstrich. Maximal 39 Zeichen sind möglich.

   Type: Wählen Sie im Drop-down-Menü **IPSec User Group** aus.

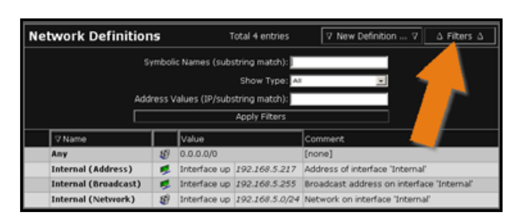
   DN Template: Für den VPN-ID-Type **Distinguished Name** benötigen Sie die folgenden Daten aus dem X.509-Verzeichnisbaum: Country (C), State (ST), Local (L), Organization (O), Unit (OU), Common Name (CN) und E-Mail Address (E).
   Die Daten müssen in diesem Eingabefeld in der gleichen Reihenfolge wie im Zertifikat aufgeführt sein.

   Comment: Über das Eingabefeld können Sie optional einen Kommentar für die IPSec-Benutzergruppe hinzufügen.

4. Speichern Sie die IPSec-Benutzergruppe durch einen Klick auf die Schaltfläche **Add Definition**.

Nach erfolgreicher Definition wird die neue **IPSec-Benutzergruppe** in die Netzwerktabelle eingetragen. Sie finden diese IPSec-Netzwerkgruppe jetzt unter seinem Namen auch in verschiedenen anderen Menüs wieder.

Filters



Mit der Funktion **Filters** können Sie aus der Tabelle *Netzwerke* (*Networks*) oder Hosts mit bestimmten Attributen herausfiltern. Diese Funktion erleichtert das Managen von großen Netzwerken erheblich, da Netzwerke eines bestimmten Typs übersichtlich dargestellt werden können.

Netzwerke filtern:

1. Klicken Sie auf die Schaltfläche **Filters**.

   Anschließend wird das Eingabefenster geöffnet.

2. Tragen Sie in den nachfolgend aufgeführten Feldern die Attribute für den Filter ein. Es müssen nicht alle Attribute definiert werden.

   Name: Falls Sie Netzwerke mit Namen filtern möchten, tragen Sie den Begriff in das Eingabemenü ein.

   Type: Mit diesem Drop-down-Menü filtern Sie Netzwerke eines bestimmten Typs.

   Address Values: Falls Sie Netzwerke mit bestimmten Adressen filtern möchten, tragen Sie in das Eingabefeld die IP-Adresse ein.

3. Um den Filter zu starten klicken Sie auf die Schaltfläche **Apply Filters**.

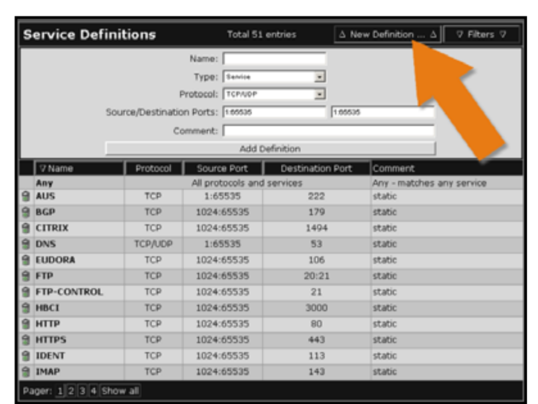
Anschließend werden nur die gefilterteten Netzwerke in der Tabelle angezeigt. Nach dem nächsten Öffnen des Menüs wird wieder die vollständige Netzwerktabelle dargestellt.

Weitere Funktionen

Definition editieren: Durch einen Klick auf die Einstellungen in den Spalten **Name**, **Value** und **Comment** öffnet sich ein Editierfenster. Anschließend können Sie die Eingaben bearbeiten.

Definition löschen: Durch einen Klick auf das Papierkorb-Symbol wird die Definition aus der Tabelle gelöscht.

5.2.2. Services



Im Menü **Services** werden die *Dienste* (*Services*) und die *Dienstgruppen* (*Service Groups*) definiert.

Dienste (**Services**) sind Definitionen für den Datenverkehr über Netzwerke, z. B. das Internet. Eine Dienstedefinition besteht aus **Namen**, **Protokollen** und **Ports**.

Folgende Protokolle stehen Ihnen zur Verfügung: *TCP*, *UDP*, *TCP/UDP*, *ICMP*, *ESP*, *AH* und *IP*.

UDP verwendet Ports von 0 bis einschließlich 65535 und ist ein Protokoll, das kein sog. ACK-Bit benötigt. UDP arbeitet besonders beim Versenden kleinerer Datenmengen schneller als **TCP**. Verlorene Pakete können über *UDP* nicht erkannt und neu angefordert werden, da es sich um ein verbindungsloses Protokoll handelt. Der Erhalt der Datenpakete wird vom Empfänger nicht quittiert.

TCP-Verbindungen benutzen ebenfalls die Ports von 0 bis 65535. Verlorene Pakete können über *TCP* erkannt und neu angefordert werden. Bei *TCP* werden alle Datenpakete vom Empfänger quittiert (verbindungsorientiertes Protokoll). Eine *TCP*-Verbindung wird zu Beginn mit

dem sog. **Three Way Handshake**-Verfahren aufgebaut und nach dem Transfer wieder abgebaut.

Die Protokolle **AH** und **ESP** werden für **Virtual Private Network** (**VPN**) benötigt. Diese Protokolle werden im Kapitel 5.7 ab Seite 355 beschrieben.

Die definierten Dienste und Gruppen werden in der Dienstetabelle aufgelistet. Per Default befinden sich in der Tabelle bereits statisch eingetragene Dienste (Services).

Die **Dienste** (**Services**) lassen sich zu **Dienstgruppen** (**Service Groups**) zusammenfassen. Diese Dienstgruppen werden behandelt wie einzelne Dienste und können wieder Teil einer übergeordneten Gruppe sein. In der Dienstetabelle sind die Dienstgruppen durch das Gruppensymbol ( ) gekennzeichnet.
Die Definition einer *Dienstgruppe* (*Service Group*) wird ab Seite 144 beschrieben.

Dienst hinzufügen:

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Service**.

2. Klicken Sie auf die Schaltfläche **New Definition**.

   Anschließend wird das Eingabefenster geöffnet.

3. Führen Sie die folgenden Einstellungen durch:

   Name: Tragen Sie in das Eingabefeld einen eindeutigen Namen für den **Dienste** (**Services**) ein.

   > Diesen Namen verwenden Sie später, z. B. um Paketfilterregeln zu setzen. Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9, Minus- und Leerzeichen sowie Unterstrich. Maximal 39 Zeichen sind möglich.

   Type: Wählen Sie im Drop-down-Menü **Service** aus.

   Protocol: Wählen Sie im Drop-down-Menü das Protokoll aus.

Source/Destination Ports: Tragen Sie in das linke Eingabemenü den Source-Port, d. h. die Client-Seite des Dienstes ein. In das rechte Eingabemenü tragen Sie den Destination-Port, d. h. die Server-Seite des Dienstes fest.

4. Die weiteren Einstellungen richten sich nun nach dem ausgewählten Protokoll:

   Für die Protokolle **TCP** und **UDP** benötigen Sie die folgenden zwei Werte. Eingabe-Optionen: Einen einzelnen Port (z. B. 80) oder eine Portrange (z. B. 1024:64000).

   Source/Destination Ports: Tragen Sie in das linke Eingabemenü den Source-Port, d. h. die Client-Seite des Dienstes ein. In das rechte Eingabemenü tragen Sie den Destination-Port, d. h. die Server-Seite des Dienstes fest.

   Die Protokolle **AH** und **ESP** werden für **IPSec VPN**-Verbindungen benötigt. Der hier eingetragene Wert muss zuvor mit der Gegenstelle des IPSec VPN-Tunnels abgesprochen werden.

   SPI: Tragen Sie hier einen Wert zwischen 256 und 65535 ein. Die Werte bis einschließlich 255 sind vom **Internet Assigned Numbers Authority (IANA)** reserviert.

   Für das Protokoll **ICMP** können Sie im Auswahlmenü **ICMP Type** die darin enthaltene Nachricht auswählen.

   Für das Protokoll **IP** tragen Sie in das Eingabefeld **Protocol Number** die Protokollnummer ein.

   Comment: Über das Eingabefeld können Sie optional einen Kommentar für den Dienst hinzufügen.

5. Speichern Sie den **Dienste** (**Services**) durch einen Klick auf die Schaltfläche **Add Definition**.

Nach erfolgreicher Definition wird der neue **Dienst** (**Services**) in die Diensttabelle eingetragen. Sie finden diesen Dienst jetzt unter seinem Namen auch in verschiedenen anderen Menüs wieder.

Dienstgruppe definieren:

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Services**.

2. Klicken Sie auf die Schaltfläche **New Definition**.

   Anschließend wird das Eingabefenster geöffnet.

3. Führen Sie die folgenden Einstellungen durch:

   Name: Tragen Sie in das Eingabefeld einen eindeutigen Namen für die **Dienstgruppe** (**Service Group**) ein.

   > Diesen Namen verwenden Sie später, z. B. um Paketfilterregeln zu setzen. Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9, Minus- und Leerzeichen sowie Unterstrich. Maximal 39 Zeichen sind möglich.

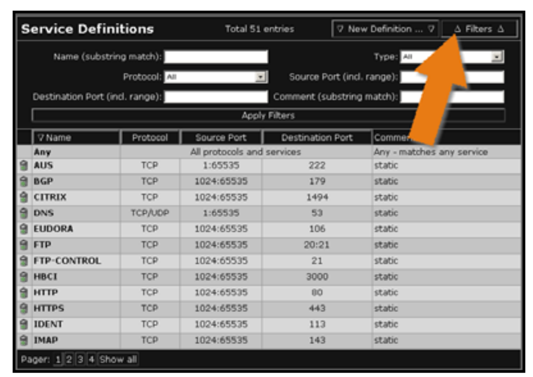
   Type: Wählen Sie im Drop-down-Menü **Service Group** aus.

   Initial Members: Wählen Sie im Auswahlfeld die Dienste aus, indem Sie auf der Tastatur die **Strg**-Taste gedrückt halten und mit der Maus die Namen markieren.

4. Speichern Sie die **Dienstgruppe** (**Service Group**) durch einen Klick auf die Schaltfläche **Add Definition**.

Nach erfolgreicher Definition wird die neue **Dienstgruppe** (**Service Group**) in die Tabelle eingetragen. Sie finden diese Dienstgruppe jetzt unter seinem Namen auch in verschiedenen anderen Menüs wieder.

Filters



Mit der Funktion **Filters** können Sie aus der Tabelle *Dienste* (*Services*) mit bestimmten Attributen herausfiltern. Diese Funktion erleichtert das Managen von großen Netzwerken mit vielen Diensten erheblich, da Dienste eines bestimmten Typs übersichtlich dargestellt werden können.

Dienste filtern:

1. Klicken Sie auf die Schaltfläche **Filters**.

   Anschließend wird das Eingabefenster geöffnet.

2. Tragen Sie in den nachfolgend aufgeführten Feldern die Attribute für den Filter ein. Es müssen nicht alle Attribute definiert werden.

   Name: Falls Sie Dienste mit bestimmten Namen filtern möchten, tragen Sie den Begriff in das Eingabemenü ein.

   Type: Mit diesem Drop-down-Menü filtern Sie Dienste eines bestimmten Typs.

   Protocol: Mit diesem Drop-down-Menü filtern Sie Dienste mit bestimmten Protokollen.

   Source Port: Falls Sie Dienste mit einem bestimmten Quellport filtern möchten, tragen Sie diesen in das Eingabefeld ein.

   Destination Port: Falls Sie Dienste mit einem bestimmten Zielport filtern möchten, tragen Sie diesen in das Eingabefeld ein.

Comment: Falls Sie Dienste mit bestimmten Kommentaren filtern möchten, tragen Sie die Begriffe in das Eingabemenü ein.

3. Um den Filter zu starten klicken Sie auf die Schaltfläche **Apply Filters**.

Anschließend werden nur die gefilterteten Dienste in der Tabelle angezeigt. Nach dem nächsten Öffnen des Menüs wird wieder die vollständige Diensttabelle dargestellt.

Weitere Funktionen

Definition editieren: Durch einen Klick auf die Einstellungen in den Spalten **Name**, **Value** und **Comment** öffnet sich ein Editierfenster. Anschließend können Sie die Eingaben bearbeiten.

Definition löschen: Durch einen Klick auf das Papierkorb-Symbol wird die Definition aus der Tabelle gelöscht.

5.2.3. Users



In Menü **Users** werden die **lokalen Benutzer** (**Local Users**) hinzugefügt, wenn der Gebrauch der Proxydienste nach Personen eingeschränkt werden soll. Dies ist die Alternative dazu, eine externe Benutzerdatenbank abzufragen. Anschließend können Sie diesen lokalen Benutzern in der Benutzertabelle den Zugriff auf die Dienste **HTTP**-Proxy, **SMTP**-Proxy, **SOCKS**-Proxy, **WebAdmin**, **L2TP over IPSec** und **PPTP** (Remote Access) erlauben.



Sicherheitshinweis:

Standardmäßig hat nur der Benutzer **admin** Zugriff auf das Konfigurationstool **WebAdmin**. Sie sollten das Passwort zum Konfigurationstool in regelmäßigen Abständen ändern.

Lokalen Benutzer hinzufügen:

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Users**.

2. Klicken Sie auf die Schaltfläche **New Definition**.

   Anschließend wird das Eingabefenster geöffnet.

3. Führen Sie die folgenden Einstellungen durch:

   Username: Tragen Sie in das Eingabefeld einen eindeutigen Namen für den **Lokalen Benutzer** (**Local User**) ein.

   > Diesen Benutzernamen verwenden Sie später, z. B. um Paketfilterregeln zu setzen. Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9, Minus- und Leerzeichen sowie Unterstrich. Maximal 39 Zeichen sind möglich.

   Password: Tragen Sie in das Eingabefeld das Passwort ein.



Sicherheitshinweis:

Setzen Sie sichere Passwörter! Ihr Vorname rückwärts buchstabiert ist beispielsweise kein ausreichend sicheres Passwort – besser wäre z. B. xfT35!4z.

   Comment: Über das Eingabefeld können Sie optional einen Kommentar für den lokalen Benutzer hinzufügen.

4. Speichern Sie den **Lokalen Benutzer** (**Local User**) durch einen Klick auf die Schaltfläche **Add Definition**.

   Der neue *Benutzer* (*User*) wird anschließend in der Tabelle angezeigt.

5. Schalten Sie in der Tabelle für den **Lokalen Benutzer** (**Local User**) die Dienste frei.

   Zu Beginn sind für den Benutzer noch keine Dienste freigeschalten. Sie schalten den Dienst ein, indem Sie auf den entsprechenden Begriff klicken.

   Beispiel:

   ~~HTTP~~ = der HTTP-Proxy ist nicht freigeschaltet

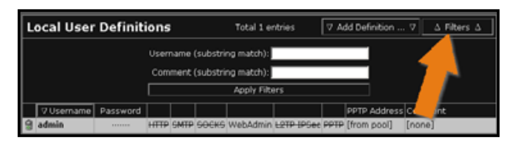
HTTP = der HTTP-Proxy ist freigeschaltet

Die möglichen Dienste sind: **HTTP**-Proxy, **SMTP**-Proxy, **SOCKS**-Proxy, **WebAdmin**, **L2TP over IPSec** und **PPTP** (Remote Access).

PPTP Address: Bei PPTP-Verbindungen kann den Remote Hosts anstatt einer dynamischen Adresse aus einem PPTP IP Pool auch eine statische IP-Adresse zugewiesen werden. Um eine statische IP zu definieren klicken Sie auf das Feld in der Spalte *PPTP Address* und tragen in das Eingabefeld die Adresse ein.
Mit einem Klick auf die Schaltfläche **Save** werden die Änderungen gespeichert. Um den Vorgang abzubrechen klicken Sie auf die Schaltfläche **Cancel**.

Weitere Informationen zu **PPTP VPN Access** finden Sie im Kapitel 5.3.7 ab Seite 212.

Filters



Mit der Funktion **Filters** können Sie aus der Tabelle *lokale Benutzer* (*local Users*) mit bestimmten Attributen herausfiltern. Diese Funktion erleichtert das Managen von großen Netzwerkkonfigurationen erheblich, da Benutzer eines bestimmten Typs übersichtlich dargestellt werden können.

Lokale Benutzer filtern:

1. Klicken Sie auf die Schaltfläche **Filters**.

   Anschließend wird das Eingabefenster geöffnet.

2. Tragen Sie in den nachfolgend aufgeführten Feldern die Attribute für den Filter ein. Es müssen nicht alle Attribute definiert werden.

Username: Falls Sie Benutzer nach Benutzernamen filtern möchten, tragen Sie den Begriff in das Eingabemenü ein.

Comment: Falls Sie Benutzer mit bestimmten Kommentaren filtern möchten, tragen Sie die Begriffe in das Eingabemenü ein.

3. Um den Filter zu starten klicken Sie auf die Schaltfläche **Apply Filters**.

Anschließend werden nur die gefilterteten Benutzer in der Tabelle angezeigt. Nach dem nächsten Öffnen des Menüs wird wieder die vollständige Benutzertabelle dargestellt.

Weitere Funktionen

Lokalen Benutzer editieren: Durch einen Klick auf die Einstellungen in den Spalten **Name**, **Password**, **PPTP Address** und **Comment** öffnet sich ein Editierfenster. Anschließend können Sie die Eingaben bearbeiten.

Lokalen Benutzer löschen: Durch einen Klick auf das Papierkorb-Symbol wird die Definition aus der Tabelle gelöscht.

5.2.4. Time Events

Im Menü **Time Events** werden **einzelne** (**single**) oder **periodisch stattfindende** (**Recurring**) Zeitintervalle definiert.

Time Events		Total 4 entries				New event definition
∇ Name	Type	Start Time		Stop Time		Weekdays
After_Hours	Recurring	18:00		23:59		All (Daily Recurring)
Test	Single	2005-06-07	00:00	2005-06-08	23:59	
Weekend	Recurring	00:00		23:59		Sat, Sun
Workdays	Recurring	06:00		23:59		Mon, Tue, Wed, Thu, Fri

Diese definierten *Time-Events* können bei den folgenden Modulen genutzt werden:

- Im **Paketfilter** (**Packet Filter**) können die Regeln für den Datenverkehr für bestimmte Zeitintervalle definiert werden.
- Im **Content Filter** (**Surf Protection**) können in der Tabelle **Profile Assignment** für den Zugriff auf den HTTP-Proxy Zeitintervalle zugeteilt werden.

Es können zwei Time-Event-Typen definiert werden:

- **Recurring**: Das eingestellte Zeitintervall wiederholt sich periodisch. Der Beginn und das Ende werden durch Uhrzeitangaben definiert. Das periodische Intervall wird durch Angabe der Wochentage festgesetzt.
- **Sinle**: Das eingestellt Zeitintervall findet nur einmal statt. Der Beginn und das Ende werden durch Datums- und Uhrzeitangaben definiert. Wochentage können hier nicht eingestellt werden.

Zeitintervall definieren:

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Time Events**.
2. Klicken Sie auf die Schaltfläche **New event definition**.

   Anschließend wird eine neue Zeile in der Tabelle angezeigt.
3. Führen Sie die folgenden Einstellungen durch:

   Name: Tragen Sie in das Eingabefeld einen eindeutigen Namen für den **Zeitintervall** (**Time Event**) ein.

   > Diesen Namen verwenden Sie später, z. B. um Paketfilterregeln zu setzen. Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9, Punkt, Minus- und Leerzeichen sowie Unterstrich. Maximal 39 Zeichen sind möglich.

   Type: Wählen Sie im Drop-down-Menü den Typ aus.

   Start Time: Stellen Sie hier den Beginn des Intervalls ein. Durch einen Klick auf das Feld werden die Eingabefenster geöffnet.

   Stop Time: Stellen Sie hier das Ende des Intervalls ein. Durch einen Klick auf das Feld werden die Eingabefenster geöffnet.

   Weekdays: Für den Zeitintervalltyp Recuring stellen Sie hier die Wochentage ein, für die das Zeitintervall bestimmt ist. Durch einen Klick auf das Feld werden die Optionsfelder zu Auswahl der Wochentage angezeigt.

Die neue Definition ist sofort aktiv und kann in den Modulen mit einer entsprechenden Time-Event-Funktion ausgewählt werden.

Weitere Funktionen

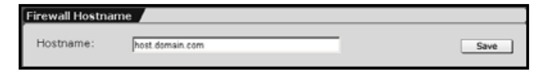
Zeitintervall löschen: Durch einen Klick auf das Papierkorb-Symbol wird die Definition aus der Tabelle gelöscht.

5.3. Netzwerkeinstellungen (Network)

Im Verzeichnis **Network** konfigurieren Sie die **Netzwerkkarten** und **virtuellen Schnittstellen** (**Interfaces**) und führen netzwerkspezifische Einstellungen durch.

5.3.1. Hostname/DynDNS

Firewall Hostname



Hostname: Tragen Sie in das Eingabenfeld den Hostnamen für das Internet-Sicherheitssystem ein.
Beispiel: FIREWALL.meinedomain.com

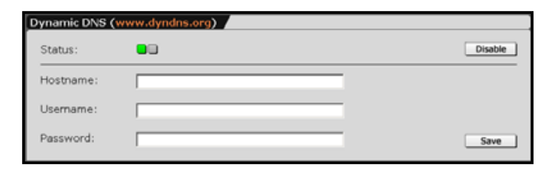
Ein Hostname, bzw. Domainname darf aus alphanumerischen Zeichen sowie Punkt- und Minus-Zeichen bestehen. Am Ende muss ein alphabetischer Bezeichner vorhanden sein, z. B. „com“, „de“ oder „org“. Der **Hostname** wird in allen **Notification E-Mails** in der Betreffzeile angezeigt.

Speichern Sie anschließend Ihre Eingabe durch einen Klick auf die Schaltfläche **Save**.

Hinweis:

In allen **Notification E-Mails** an den Administrator wird in der Betreffzeile der **Hostname** angezeigt.

Dynamic DNS



Mit **Dynamic DNS** wird ein Gerät oder eine VPN-Gegenstelle über einen DNS-auflösbaren Namen angesprochen. Zu diesem Namen wird auf einem öffentlichen DNS-Server im Internet bei jedem Verbindungsaufbau die jeweils gültige IP-Adresse hinterlegt. Unter diesem Namen kann ein Host immer erreicht werden - natürlich nur sofern er online ist. Mit Dynamic DNS kann z. B. ein mobiler Nutzer auf sein Firmennetz zuzugreifen, selbst wenn die Firma nur über einen Standard-DSL-Anschluss mit dynamischer IP-Adresse verfügt. Neben VPN-Anwendungen eignet sich *Dynamic DNS* auch für Fernwartung und Fernüberwachung.

Dynamic-DNS-Server definieren:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Hostname/ DynDNS**.

2. Schalten Sie die Funktion in der Spalte **Status** durch einen Klick auf die Schaltfläche **Enable** ein.

   Anschließend wird das Eingabefenster geöffnet.

3. Führen Sie die folgenden Einstellungen durch:

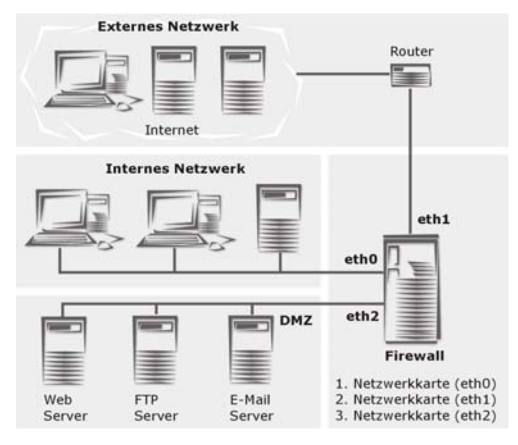
   Hostname: Tragen Sie in das Eingabenfeld den Hostnamen ein.

   Username: Tragen Sie in das Eingabenfeld den Benutzernamen ein.

   Password: Tragen Sie in das Eingabefeld das Passwort ein.

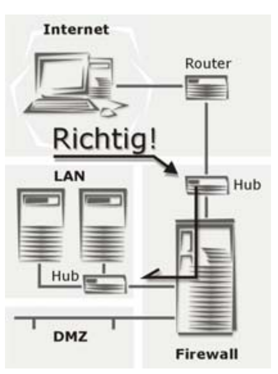
4. Speichern Sie Ihre Eingabe durch einen Klick auf die Schaltfläche **Save**.

5.3.2. Interfaces

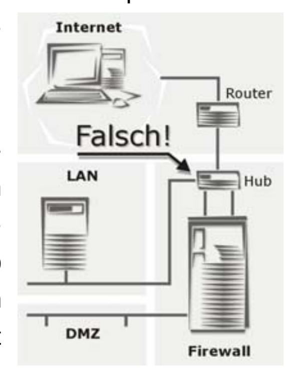


Um ein internes Netzwerk (LAN) vor einem externen Netzwerk (Internet) zu sichern, benötigt eine Firewall mindestens zwei **Netzwerkkarten**. In unseren Beispielen ist die **Netzwerkkarte eth0** immer die Schnittstelle zum internen Netzwerk. Die **Netzwerkkarte eth1** ist die Schnittstelle zum externen Netzwerk (Internet). Diese beiden Seiten werden auch **Trusted** und **Untrusted** genannt.

Während der Installation werden die Netzwerkkarten automatisch erkannt. Falls später weitere Netzwerkkarten hinzugefügt werden, ist eine Neu-Installation des Internet-Sicherheitssystems notwendig. Verwenden Sie die Backup-Funktion, um nach der Neu-Installation Ihre alte System-Konfiguration wieder einzuspielen.



Die Firewall muss, wie in der linken Grafik dargestellt, die Schnittstelle zwischen dem LAN und dem Internet sein. Alle Datenpakete müssen das Internet-Sicherheitssystem passieren.



Wir raten dringend davon ab, die Schnittstellen der Firewall, wie in der rechten Grafik dargestellt, über einen Hub oder Switch physikalisch zusammen auf ein Netzwerksegment zu legen, wenn dieser nicht

als VLAN-Switch konfiguriert ist. Unter Umständen kann es dann zu falschen ARP-Auflösungen (Address Resolution Protocol) kommen (ARP-Clash), die nicht alle Betriebssysteme (z. B. die von Microsoft) verwalten können. Pro Firewall-Netzwerk-Schnittstelle muss daher auch ein physikalisches Netzwerk-Segment verwendet werden.

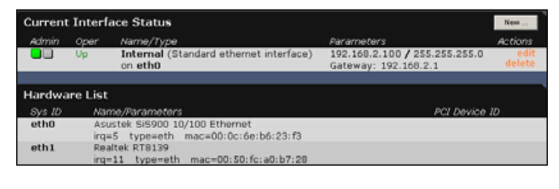
Im Menü **Interfaces** verwalten Sie alle auf dem Internet-Sicherheitssystem installierten Netzwerkkarten und konfigurieren die Schnittstelle zum externen Netzwerk (Internet) sowie die Schnittstellen zu den internen Netzwerken (LAN, DMZ).

Hinweis:

Beachten Sie bei der Planung und Konfiguration der Schnittstellen, welche Netzwerkkarten Sie jeweils auf dem Sicherheitssystem auswählen. Für die Schnittstelle zum externen Netzwerk (Internet) wird in der Regel die Netzwerkkarte mit der Sys ID **eth1** verwendet.
Für eine spätere Installation des **High Availability (HA)**-Systems benötigen Sie auf beiden Systemen eine Netzwerkkarte mit gleicher **Sys ID**. Die Installation des **HA**-Systems wird in Kapitel 5.1.11 ab Seite 122 beschrieben.

In den nachfolgenden Abschnitten wird erklärt, wie die verschiedenen Schnittstellen-Typen (**Interface Types**) über die Fenster **Current Interface Status** und **Hardware List** verwaltet und konfiguriert werden.

Current Interface Status



In diesem Fenster konfigurieren Sie die Netzwerkkarten und virtuellen Schnittstellen (**Interfaces**). In der Tabelle werden alle bereits konfigurierten Netzwerkkarten angezeigt. Das linke Bild zeigt das Menü **Interfaces** nach der Installation der Software mit drei eingebauten Ethernet-Netzwerkkarten.

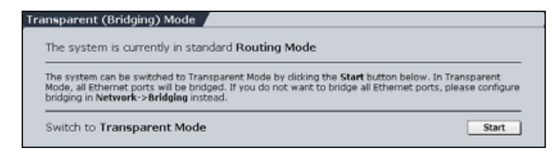
Während der Installation wurde die Schnittstelle mit der Bezeichnung **eth0** bereits konfiguriert. Sie ist die Schnittstelle zwischen dem Internet-Sicherheitssystem und dem internen Netzwerk (LAN). Per Default wird dieser Netzwerkkarte der Namen **Internal** zugewiesen. In der Tabelle sind alle Informationen zu den konfigurierten Schnittstellen enthalten: Schnittstelle ein/aus (Statusampel zeigt **Grün**/**Rot**), der aktuelle Funktionszustand (**Up**/**Down**), Name (**Name**), Bezeichnung (**Sys ID**) und Schnittstellen-Typ (**eth**/**ttyS**) sowie IP-Adresse und Netzwerkmaske (**Parameters**).
Durch einen Klick auf die Statusampel in der Spalte **Admin** wird die Schnittstelle ein- und ausgeschaltet. Mit den Funktionen in der Spalte **Actions** können Sie die Schnittstellen bearbeiten (**edit**) oder entfernen (**delete**).

Bei diesem Internet-Sicherheitssystem weisen Sie jeder virtuellen Schnittstelle einen **Namen** und eine bestimmte Netzwerkkarte zu. Für jede konfigurierte Schnittstelle werden anschließend automatisch drei logische Netzwerke definiert:

- Eine Schnittstelle (**NAME (Address)**), bestehend aus der von Ihnen definierten IP-Adresse und der Netzwerkmaske 255.255.255.255 (Host)
- Ein Netzwerk (**NAME (Network)**), bestehend aus der Netzwerk-IP-Adresse und der Netzwerkmaske (Netzwerk)
- Broadcast (**NAME (Broadcast)**), bestehend aus der Broadcast-IP und der Netzwerkmaske 255.255.255.255 (Host)

Die Netzwerke werden im Menü **Networks** angezeigt. Wenn bei einer Netzwerkkarte eine dynamische IP-Adressenverteilung, z. B. bei **DHCP** oder **PPPoE** verwendet wird, werden diese Einstellungen automatisch aktualisiert. Alle Funktionen die sich auf diese Einstellungen beziehen (z. B. Paketfilter oder NAT), erhalten automatisch die geänderte IP-Adresse.

Transparent (Bridging) Mode

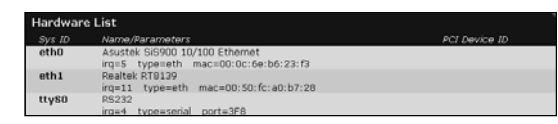


Mit der Funktion **Transparent (Bridging) Mode** werden alle konfigurierten Netzwerkkarten entfernt und eine Bridge-Schnittstelle wird definiert. Diese Schnittstelle enthält die Adresse von der Netzwerkkarte mit dem Default Gateway. Falls kein Default Gateway vorhanden ist, wird vom Sicherheitssystem die erste IP-Adresse verwendet, die auf einer Ethernet-Netzwerkkarte definiert wurde.

Die Funktion **Transparent (Bridging) Mode** entspricht der Funktion **Bridging** im Menü **Network/Interfaces**. Weitere Informationen erhalten Sie in Kapitel 5.3.3 auf Seite 191.

Auf den **Routing Mode** können Sie wieder zurückschalten, indem Sie nochmals auf die Schaltfläche **Start** klicken. Die Bridge wird anschließend in ein *Standard Ethernet Interface* geändert. Diese Schnittstelle enthält alle Adress-Einstellungen von der *Bridge*.

Hardware List



Hardware List

Sys ID	Name/Parameters	PCI Device ID
eth0	Asustek SiS900 10/100 Ethernet irq=5 type=eth mac=00:0c:6e:b6:23:f3	
eth1	Realtek RT8139 irq=11 type=eth mac=00:50:fc:a0:b7:28	
ttyS0	RS232 irq=4 type=serial port=3F8	

In dieser Tabelle sind alle auf dem Internet-Sicherheitssystem installierten Netzwerkkarten und verfügbaren **seriellen Schnittstellen** mit den entsprechenden Hardware-Informationen enthalten, z. B. die vom System zugewiesene Bezeichnung (**Sys ID**), der Netzwerkarten-Typ, die MAC-Hardware-Adresse (**Name/Parameters**) sowie Angaben zum PCI-Bus: Bus/Gerät/ Funktion (**PCI Device ID**).

An die serielle Schnittstelle können PPP-Modems, die auf der seriellen Konsole aufsetzen angeschlossen werden. Die Konfiguration der seriellen Schnittstelle mit einem PPP-Modem wird in Kapitel 5.3.2.6 ab Seite 185 beschrieben.

Fehler:

Die Tabelle **Hardware List** entählt nicht alle Netzwerkkarten.

Mögliche Fehlerursachen:

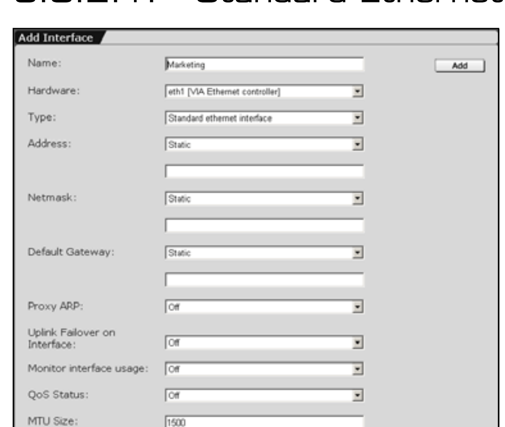


Die fehlende Netzwerkkarte wurde erst nach Installation des Internet-Sicherheitssystems eingebaut oder sie wurde während der Installation nicht erkannt. Setzen Sie sich in diesem Fall mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

Achtung:

Wenn Sie die **IP-Adresse** der internen Netzwerkkarte **eth0** ändern, besteht die Möglichkeit, dass Sie keine Verbindung mehr zum Internet-Sicherheitssystem bekommen.

5.3.2.1. Standard Ethernet Interface



Für eine Standard-Ethernet-Schnittstelle zu einem internen oder externen Netzwerk muss auf der Netzwerkkarte die primäre Netzwerkkartenadresse eingerichtet werden.

Alle auf dem Sicherheitssystem installierten Netzwerkkarten werden in der Tabelle **Hardware List** angezeigt.

Standard-Ethernet-Netzwerkkarte einrichten:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Interfaces**.

2. Klicken Sie auf die Schaltfläche **New**.

   Das Fenster **Add Interface** wird geöffnet.

3. Tragen Sie in das Eingabefeld **Name** den Namen der Schnittstelle ein. (Beispiel: **External** für eine Verbindung zum Internet)

4. Wählen Sie im Drop-down-Menü **Hardware** die Netzwerkkarte aus.

Tipp:

Wählen Sie als Schnittstelle zum *externen Netzwerk (Internet)* die Netzwerkkarte mit der *Sys ID* **eth1** aus.

5. Wählen Sie im Drop-down-Menü **Type** den Schnittstellen-Typ **Standard Ethernet interface** aus.

   Beachten Sie, dass einer Netzwerkkarte nicht gleichzeitig der Typ **Standard Ethernet Interface** und **PPP over Ethernet**

(PPPoE-DSL) Connection oder **PPPTP over Ethernet (PPPoA-DSL) Connection** zugewiesen werden kann.

6. Führen Sie nun die spezifischen Einstellungen für den Schnitt-stellen-Typ durch:

   Address: Falls Sie eine statische IP-Adresse eintragen möchten, wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Adresse ein. Wenn Sie die Adresse durch einen DHCP-Server zuweisen lassen möchten, wählen Sie im Drop-down-Menü **Assign by DHCP** aus.

   Wichtiger Hinweis:

   Falls Sie für diese Netzwerkkarte die Ausfallsicherung **Uplink Failover on Interace** konfigurieren möchten, beachten Sie bei der Eingabe des Netzwerks die Beschreibung zu dieser Funktion!

   Netmask: Falls Sie eine statische Netzwerkmaske eintragen möchten, wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Netzwerkmaske ein. Wenn Sie die Netz-werkmaske durch einen DHCP-Server zuweisen lassen möchten, wählen Sie im Drop-down-Menü **Assign by DHCP** aus.

   Default Gateway: Bei einem statischen Default Gateway wäh-len Sie im Drop-down-Menü **Static** aus und tragen in das Ein-gabefeld die Adresse ein. Wenn Sie die Adresse durch einen DHCP-Server zuweisen lassen möchten, wählen Sie im Drop-down-Menü **Assign by DHCP** aus. Falls Sie kein Default Gate-way definieren möchten, wählen Sie im Drop-down-Menü **None** aus.

   Proxy ARP: Wenn diese Funktion aktiviert ist, wird das Internet-Sicherheitssystem auf der entsprechenden Netzwerkkarte das ARP-Protokoll für alle ihm bekannten Netzwerke setzen. Dies be-deutet, dass das System, stellvertretend für alle anderen direkt angeschlossenen Netzwerke, Pakete aus dem angeschlossenen Netzwerk annehmen und weiterleiten wird.
   Diese Funktion wird in einigen Spezialfällen benötigt, um z. B.

ein Netzwerk über das Sicherheitssystem weiterzureichen, falls es nicht möglich ist, korrekte Routen für dieses Netzwerk zu setzen. Dies kann der Fall sein, wenn Sie keinen Zugriff auf den Router Ihres Internet-Providers haben.

Per Default ist **Proxy ARP** ausgeschaltet (**Off**). Sie schalten die Funktion ein, indem Sie im Drop-down-Menü **On** auswählen.

Uplink Failover on Interface: Diese Funktion wird nur angezeigt, wenn im Drop-down-Menü **Default Gateway** die Einstellung **Assign by DHCP** oder **Static** ausgewählt wurde.

Falls es sich bei dieser Netzwerkkarte um eine Schnittstelle zum Internet (z. B. 2 Megabit Festverbindung) handelt, können Sie mit Hilfe eines zweiten Internetzugangs (z. B. DSL-Verbindung) und einer zusätzlichen Netzwerkkarte eine Ausfallsicherung einrichten. Bei einem Ausfall der **primären Verbindung** (**Primary Interface**) erfolgt dann der Uplink automatisch über den Ersatzinternetzugang. Zur Überprüfung der Verbindung werden über die *primäre Netzwerkkarte* alle fünf Sekunden vier Ping-Anfragen an die **Uplink Failover check IP** gesendet. Erst wenn alle vier Ping-Anfragen nicht beantwortet werden, wird die Ersatznetzwerkkarte geladen.

Währenddem die Internetverbindung über die *Ersatznetzwerkkarte* (*Backup Interface*) erfolgt, werden die Ping-Anfragen weiter über die *primäre Netzwerkkarte* (*Primary Interface*) verschickt. Sobald das Sicherheitssystem wieder entsprechende Antwortpakete empfängt, erfolgt die Internetverbindung wieder über die *primäre Netzwerkkarte*.

Wichtiger Hinweis:

Für die Funktion **Uplink Failover on Interface** müssen auf der Primär- und auf der Ersatznetzwerkkarte zwei unterschiedliche Netzwerke definiert werden. Sie benötigen daher neben der zusätzlichen Netzwerkkarte für die Ersatzschnittstelle zwei separate Internetzugänge.

Per Default ist **Uplink Failover on Interface** ausgeschaltet (**Off**). Wenn diese Netzwerkkarte die primäre Verbindung zum Internet sein soll, stellen Sie im Drop-down-Menü **Primary Interface** ein. Falls diese Netzwerkkarte die Standby-Verbindung enthalten soll, wählen Sie die Einstellung **Backup Interface** aus.

Uplink Failover check IP: Dieses Eingabefeld wird angezeigt, wenn bei der Funktion **Uplink Failover on Interface** die Einstellung **Primary Interface** ausgewählt ist. Geben Sie hier die IP-Adresse eines Hosts ein, der auf ICMP-Ping-Anfragen antwortet und zudem ständig erreichbar ist! Falls das System von dieser Adresse keine entsprechende Antwort erhält, wird durch die Ausfallsicherung die Backup-Schnittstelle aktiviert. In diesem Eingabefeld muss für die Ausfallsicherung immer eine IP-Adresse eingetragen sein!

Monitor Interface Usage: Mit Hilfe dieser Funktion wird die Bandbreite auf der Schnittstelle überwacht. Sobald die Bandbreite einen bestimmten Wert unter- oder überschreitet wird eine Notification E-Mail an den Administrator abgeschickt.

Für die Funktion *Monitor Interface Usage* muss in den Eingabefeldern **Uplink Bandwidth (kbits)** und **Downlink Bandwidth (kbits)** die jeweils maximal verfügbare Bandbreite eingetragen werden. Die Notification E-Mail an den Administrator wird abgesendet, sobald die tatsächlich vorhandene Bandbreite einen vordefinierten Grenzwert unter- oder überschreitet. Die Grenzwerte werden mit den **Notify**-Drop-down-Menüs eingestellt.
Die Einstellungen werden erst angezeigt, wenn die Funktion *Monitor Interface Usage* eingeschaltet (**On**) ist.

QoS Status: Um auf einer Schnittstelle Bandbreitenmanagement mit der Funktion **Quality of Service (QoS)** durchzuführen, muss zuvor die Schnittstelle freigegeben und konfiguriert werden. Um die Schnittstelle für die funktion **Quality of Service (QoS)** freizugeben, wählen Sie im Drop-down-Menü **On** aus.

Wichtiger Hinweis:

Für das Bandbreitenmanagement **Quality of Service (QoS)** müssen Sie die Werte **Uplink Bandwidth (kbits)** und **Downlink Bandwidth (kbits)** definieren. Die beiden Werte dienen als Rechengrundlage für das Bandbreitenmanagement. Falsche Angaben führen zu einem ungenauen Management der Datenströme. Die Funktion **Quality of Service (QoS)** wird in Kapitel 5.5.1 beschrieben.

Uplink Bandwidth (kbits): Diese Einstellung wird nur angezeigt, wenn die Funktion **QoS** oder **Monitor Interface Usage** eingeschaltet ist. In dieses Eingabemenü tragen Sie die für den Uplink verfügbare Bandbreite in vollen Kilobits ein. Diese ergibt sich aus den Werten der vorgeschalteten Schnittstelle oder Router. Bei einer Schnittstelle zum Internet ist es die Bandbreite der Internetverbindung - bei einem ADSL-Zugang beträgt die Uplink-Bandbreite z. B. 128 kBit/s, bei einer 2 Megabit Festverbindung z. B. 2048 kBit/s.

Downlink Bandwidth (kbits): Diese Einstellung wird nur angezeigt, wenn die Funktion **QoS** oder **Monitor Interface Usage** eingeschaltet ist. In dieses Eingabemenü tragen Sie die für den Downlink verfügbare Bandbreite in vollen Kilobits ein. Bei einer Schnittstelle zum Internet ist es die Bandbreite der Internetverbindung - bei einem ADSL-Zugang beträgt die Downlink-Bandbreite z. B. 768 kBit/s, bei einer 2 Megabit Festverbindung z. B. 2048 kBit/s.

Notify when uplink usage below (%): Diese Einstellung wird nur angezeigt, wenn die Funktion **Monitor Interface Usage** eingeschaltet ist. Stellen Sie mit dem Drop-down-Menü den unteren Grenzwert für den Uplink ein.

Notify when uplink usage exceeds (%): Diese Einstellung wird nur angezeigt, wenn die Funktion **Monitor Interface**

Usage eingeschaltet ist. Stellen Sie mit dem Drop-down-Menü den oberen Grenzwert für den Uplink ein.

Notify when downlink usage below (%): Diese Einstellung wird nur angezeigt, wenn die Funktion **Monitor Interface Usage** eingeschaltet ist. Stellen Sie mit dem Drop-down-Menü den unteren Grenzwert für den Downlink ein.

Notify when downlink usage exceeds (%): Diese Einstellung wird nur angezeigt, wenn die Funktion **Monitor Interface Usage** eingeschaltet ist. Stellen Sie mit dem Drop-down-Menü den oberen Grenzwert für den Downlink ein.

MTU Size: Die obere Grenze für die Größe der Datenpakete wird **MTU** bezeichnet. **MTU** steht für **Maximum Transfer Unit**. Bei Verbindungen die das Protokoll TCP/IP verwenden werden die Daten in Pakete aufgeteilt. Für diese Pakete wird eine maximale Größe bestimmt. Wenn nun diese obere Grenze zu hoch ist, kann es passieren, dass Datenpakete mit Informationen, die das Protokoll PPP over Ethernet betreffen, nicht richtig weitergeleitet und erkannt werden. Diese Datenpakete werden dann erneut verschickt. Allerdings kann die Performance auch eingeschränkt werden, wenn die obere Grenze zu niedrig definiert wird.
Beim Schnittstellen-Typ **Standard Ethernet Interface** kann ein Wert im Bereich 300 bis 10000 eingestellt werden.

Wichtiger Hinweis:

Ein MTU-Wert der größer als 1500 Byte ist, muss vom Netzwerktreiber und von der Netzwerkkarte (z. B. Gigabit-Schnittstelle) unterstützt werden.

Beim Schnittstellen-Typ **Standard Ethernet Interface** ist bereits ein MTU-Wert vordefiniert: 1500 Byte.

7. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

Das System prüft nun die IP-Adresse und die Netzwerkmaske auf semantische Gültigkeit. Anschließend wird die neue Schnittstelle (**Interface**) in die Tabelle **Current Interface Status** geladen. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot)

8. Schalten Sie die Schnittstelle durch einen Klick auf die Statusampel ein.

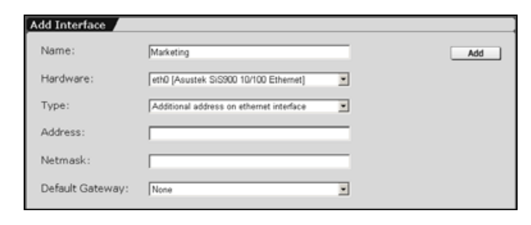
   Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). In der Spalte **Oper** wird zu Beginn die Meldung **Down** angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu laden.

9. Laden Sie das Menü neu, indem Sie auf die Schaltläche **Refresh** klicken.

   Weitere Informationen zur Funktion **Refresh** erhalten Sie in Kapitel 4.5 auf Seite 45.

Die neue Schnittstelle ist geladen, wenn die Meldung **Up** erscheint. Die Einstellungen werden in der Spalte **Parameters** angezeigt.

5.3.2.2. Additional Address on Ethernet Interface



Einer Netzwerkkarte können mehrere zusätzliche IP-Adressen zugeordnet werden (IP-Aliase). Diese Funktion wird benötigt, um auf einer Netzwerkkarte mehrere logische Netzwerke zu verwalten. Sie kann auch im Zusammenhang mit der Funktion **NAT** notwendig sein, um dem Internet-Sicherheitssystem zusätzliche Adressen zuzuweisen. Die Funktion **NAT** wird in Kapitel 5.3.5 ab Seite 198 beschrieben. Auf jeder Netzwerkkarte können bis zu 255 zusätzliche Adressen konfiguriert werden.

Zusätzliche Adresse einer Netzwerkkarte zuweisen:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Interfaces**.
2. Klicken Sie auf die Schaltfläche **New**.

   Das Fenster **Add Interface** wird geöffnet.
3. Tragen Sie in das Eingabefeld **Name** den Namen der Schnittstelle ein.
4. Wählen Sie im Drop-down-Menü **Hardware** die Netzwerkkarte aus.
5. Wählen Sie im Drop-down-Menü **Type** den Schnittstellen-Typ **Additional address on Ethernet interface** aus.
6. Führen Sie nun die spezifischen Einstellungen für den Schnittstellen-Typ durch.

   Address: Bei diesem Schnittstellen-Type kann nur eine statische IP-Adresse gesetzt werden. Tragen Sie in das Eingabefeld die Adresse ein.

Netmask: Bei diesem Schnittstellen-Type kann nur eine statische Netzwerkmaske gesetzt werden. Tragen Sie in das Eingabefeld die Netzwerkmaske ein.

Default Gateway: Wenn Sie ein Default Gateway definieren möchten wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Adresse ein. Falls Sie kein Default Gateway definieren möchten, wählen Sie im Drop-down-Menü **None** aus.

7. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

Das System prüft nun die IP-Adresse und die Netzwerkmaske auf semantische Gültigkeit. Anschließend wird die neue Schnittstelle (**Interface**) in die Tabelle **Current Interface Status** geladen. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot).

8. Schalten Sie die Schnittstelle durch einen Klick auf die Statusampel ein.

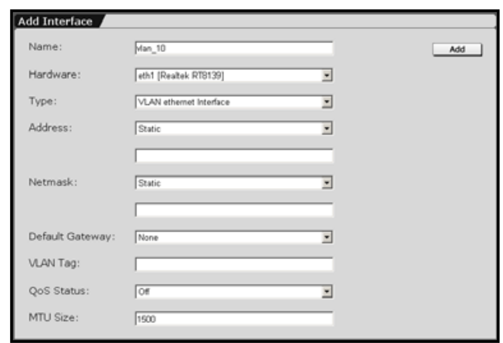
Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). In der Spalte **Oper** wird zu Beginn die Meldung **Down** angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu laden.

9. Laden Sie das Menü neu, indem Sie auf die Schaltläche **Refresh** klicken.

Weitere Informationen zur Funktion **Refresh** erhalten Sie in Kapitel 4.5 auf Seite 45.

Die neue Schnittstelle ist geladen, wenn die Meldung **Up** erscheint. Die Einstellungen werden in der Spalte **Parameters** angezeigt.

5.3.2.3. Virtual LAN



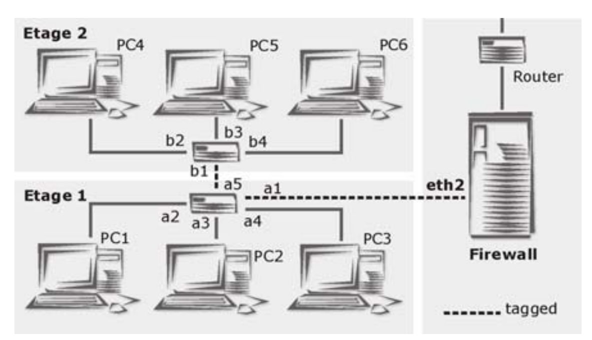
Mit **Virtual LAN** kann ein Netzwerk auf Ethernet-Ebene (Layer 2) in mehrere virtuelle Netzwerksegmente aufgeteilt werden. Dies kann z. B. aus Sicherheitsgründen von Vorteil sein, wenn bestimmte Rechner (Clients) in einem Netzwerk nicht miteinander kommunizieren dürfen. In größeren Netzwerken kann es wiederum praktisch sein, wenn weiter entfernte Rechner (Clients) im selben Netzwerksegment liegen können (Siehe Beispielkonfiguration auf der nächsten Seite).

Auf einem VLAN-fähigen Switch können die Ports in verschiedene Gruppen getrennt werden. Bei einem Switch mit 20 Ports kann z. B. das VLAN Gruppe 1 die Ports 1 bis 10 und das VLAN Gruppe 2 die Ports 11 bis 20 erhalten. Der Rechner an Port 1 kann nun nicht mehr mit dem Rechner an Port 11 kommunizieren. Der Switch wurde demnach in zwei kleinere Switches aufgeteilt.

Für die Verbindung zwischen dem Internet-Sicherheitssystem und den Virtual LANs benötigen Sie eine Netzwerkkarte mit **tag**-fähigem Treiber. Ein **Tag** ist ein kleiner 4-Byte-Header, der an den Ethernet-Header angefügt wird. Dieser angehängte Header enthält die VLAN-Nummer, mit 12 Bit. Es sind also 4095 verschiedene virtuelle LANs möglich. Diese VLAN-Nummer wird im Konfigurationstool als **VLAN Tag** bezeichnet.
Die tagged Pakete dienen nur zur Kommunikation zwischen den VLAN-fähigen Switches und dem Internet-Sicherheitssystem. Die an den Switches angeschlossenen Rechner müssen keine tag-fähigen Netzwerkkarten haben. Allerdings muss der entsprechende Port dieses Switchs als **untagged Port** definiert werden. Die VLAN-fähigen

Switches haben meist eine serielle Schnittstelle. Über diese Schnittstelle können mittels Terminalprogramm die verschiedenen Einstellungen durchgeführt werden.

Beispielkonfiguration:



Sie haben mehrere Arbeitsplätze wie in der linken Grafik dargestellt auf zwei Etagen verteilt. Die Computer jeder Etage sind jeweils an einen Switch angeschlossen. PC1 und PC2 von Etage 1 sollen nun mit PC4 von Etage 2 zum Netzwerksegment VLAN 10 zusammengefasst werden. PC3, PC5 und PC6 werden zu VLAN 20 zusammengefasst.

Auf beiden Switches müssen die Ports konfiguriert werden:

Switch a

Port	VLAN Tag	tagged/ untagged
1	10, 20	T
2 (PC1)	10	U
3 (PC2)	10	U
4 (PC3)	20	U
5	10,20	T

Switch b

Port	VLAN Tag	tagged/ untagged
1	10, 20	T
2 (PC4)	10	U
3 (PC5)	20	U
4 (PC6)	20	U

Für PC3 sieht es nun so aus, als wäre er nur über einen Switch mit PC5 und PC6 verbunden.

Damit die Rechner nun eine Verbindung zum externen Netzwerk (Internet) erhalten, muss noch die Schnittstelle zum Internet-Sicherheitssystem (im Beispiel eth2) eingestellt werden.

Achtung:

zur Konfiguration einer Schnittstelle zum **Virtual LAN** benötigen Sie eine Netzwerkkarte mit **tag**-fähigem Treiber.
Die **Hardware Compatibility List (HCL)** befindet sich auf **http://www.astaro.com/kb**. Mit Hilfe des Suchbegriffs **HCL** gelangen Sie schnell auf die entsprechende Seite.

Virtual LAN einrichten:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Interfaces**.

2. Klicken Sie auf die Schaltfläche **New**.

   Das Fenster **Add Interface** wird geöffnet.

3. Tragen Sie in das Eingabefeld **Name** den Namen der Schnittstelle ein.

4. Wählen Sie im Drop-down-Menü **Hardware** eine Netzwerkkarte aus.

5. Wählen Sie im Drop-down-Menü **Type** den Schnittstellen-Typ **VLAN Ethernet Interface** aus.

6. Führen Sie nun die spezifischen Einstellungen für den Schnittstellen-Typ **VLAN Ethernet Interface** durch.

   Address: Weisen Sie der virtuellen Schnittstelle eine IP-Adresse zu. Falls Sie eine statische IP-Adresse eintragen möchten, wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Adresse ein. Wenn Sie die Adresse durch einen DHCP-Server zuweisen lassen möchten, wählen Sie im Drop-down-Menü **Assign by DHCP** aus.

   Netmask: Falls Sie eine statische Netzwerkmaske eintragen möchten, wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Netzwerkmaske ein. Wenn Sie die Netz-

werkmaske durch einen DHCP-Server zuweisen lassen möchten, wählen Sie im Drop-down-Menü **Assign by DHCP** aus.

Default Gateway: Bei einem statischen Default Gateway wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Adresse ein. Wenn Sie die Adresse durch einen DHCP-Server zuweisen lassen möchten, wählen Sie im Drop-down-Menü **Assign by DHCP** aus. Falls Sie kein Default Gateway definieren möchten, wählen Sie im Drop-down-Menü **None** aus.

VLAN Tag: Tragen Sie in das Eingabefeld den **Tag** für das virtuelle Netzwerk ein.

QoS Status: Um auf einer Schnittstelle Bandbreitenmanagement mit der Funktion **Quality of Service (QoS)** durchzuführen, muss zuvor die Schnittstelle freigegeben und konfiguriert werden. Um die Schnittstelle für die Funktion **Quality of Service (QoS)** freizugeben, wählen Sie im Drop-down-Menü **On** aus.

Wichtiger Hinweis:

Für das Bandbreitenmanagement **Quality of Service (QoS)** müssen Sie die Werte **Uplink Bandwidth (kbits)** und **Downlink Bandwidth (kbits)** definieren. Die beiden Werte dienen als Rechengrundlage für das Bandbreitenmanagement. Falsche Angaben führen zu einem ungenauen Management der Datenströme. Die Funktion **Quality of Service (QoS)** wird in Kapitel 5.5.1 beschrieben.

Uplink Bandwidth (kbits): Diese Einstellung wird nur angezeigt, wenn die Funktion **QoS** eingeschaltet ist. In dieses Eingabemenü tragen Sie die für den Uplink verfügbare Bandbreite in vollen Kilobits ein. Diese ergibt sich aus den Werten der vorgeschalteten Schnittstelle oder Router.

Downlink Bandwidth (kbits): Diese Einstellung wird nur angezeigt, wenn die Funktion **QoS** eingeschaltet ist. In dieses Einga-

bemenü tragen Sie die für den Downlink verfügbare Bandbreite in vollen Kilobits ein.

MTU Size: Die obere Grenze für die Größe der Datenpakete wird **MTU** bezeichnet. **MTU** steht für **Maximum Transfer Unit**. Bei Verbindungen die das Protokoll TCP/IP verwenden werden die Daten in Pakete aufgeteilt. Für diese Pakete wird eine maximale Größe bestimmt. Wenn nun diese obere Grenze zu hoch ist, kann es passieren, dass Datenpakete mit Informationen, die das Protokoll PPP over Ethernet betreffen, nicht richtig weitergeleitet und erkannt werden. Diese Datenpakete werden dann erneut verschickt. Allerdings kann die Performance auch eingeschränkt werden, wenn die obere Grenze zu niedrig definiert wird.
Bei einer Ethernet-Netzwerkarte beträgt die MTU maximal 1500 Byte.

Beim Schnittstellen-Typ **VLAN Ethernet Interface** ist per Default bereits ein MTU-Wert definiert: 1500 Byte.

7. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

Das System prüft nun die IP-Adresse und die Netzwerkmaske auf semantische Gültigkeit. Anschließend wird die neue Schnittstelle (**Interface**) in die Tabelle **Current Interface Status** geladen. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot).

8. Schalten Sie die Schnittstelle durch einen Klick auf die Statusampel ein.

Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). In der Spalte **Oper** wird zu Beginn die Meldung **Down** angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu laden.

9. Laden Sie das Menü neu, indem Sie auf die Schaltläche **Refresh** klicken.

Weitere Informationen zur Funktion **Refresh** erhalten Sie in Kapitel 4.5 auf Seite 45.

Die neue Schnittstelle ist geladen, wenn die Meldung **Up** erscheint. Die Einstellungen werden in der Spalte **Parameters** angezeigt.

Die neue virtuelle Schnittstelle wird auch in der Tabelle **Hardware Device Overview** angezeigt, da dieser ebenso wie einer Standard-Ethernet-Netzwerkarte eine zusätzliche IP-Adresse zugeordnet werden kann (IP-Aliase). Die **Sys ID** dieser virtuellen Schnittstelle setzt sich aus der *Sys ID* der verwendeten Netzwerkkarte und des zugeteilten *Tag* zusammen.

5.3.2.4. PPPoE-DSL-Verbindung



Diesen Schnittstellen-Typ benötigen Sie, wenn Sie eine **DSL**-Verbindung zum Internet mit dem Protokoll **PPP over Ethernet** aufbauen möchten. Für die Konfiguration benötigen Sie die DSL-Zugangsdaten inklusive Passwort. Die Daten erhalten Sie von Ihrem Internet Service Provider.

Hinweis:

Die Installation und die nötigen Einstellungen am Internet-Sicherheitssystem speziell für den Internet-Zugang mit **T-DSL** (Telekom Deutschland) wird im Leitfaden **Netzwerk mit T-DSL** erklärt. Nachdem die Schnittstelle geladen wurde, ist das System 24 Stunden am Tag in das externe Netzwerk (Internet) eingewählt. Stellen Sie daher sicher, dass die Abrechnung bei ihrem Provider nach dem Tarif **dsl flat** erfolgt.
Sie finden den aktuellen Leitfaden unter der Internetadresse **http://www.astaro.com/kb**.

PPP over Ethernet (PPPoE-DSL) einrichten:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Interfaces**.

2. Klicken Sie auf die Schaltfläche **New**.

   Das Fenster **Add Interface** wird geöffnet.

3. Tragen Sie in das Eingabefeld **Name** den Namen der Schnittstelle ein.

4. Wählen Sie im Drop-down-Menü **Hardware** die Netzwerkkarte aus.

Tipp:

Wählen Sie als Schnittstelle zum externen Netzwerk (Internet) die Netzwerkkarte mit der Sys ID **eth1** aus.

Eine Netzwerkkarte auf der bereits die primäre Netzwerkkarten-Adresse eingerichtet wurde, kann hier nicht mehr ausgewählt werden.

5. Wählen Sie im Drop-down-Menü **Type** den Schnittstellen-Typ **PPP over Ethernet (PPPoE-DSL) Connection** aus.

Für diese Einstellungen benötigen Sie die Zugangsdaten für die DSL-Verbindung.

Address: Behalten Sie die Default-Einstellung **Assigned by remote** bei, wenn Sie keine feste IP-Adresse haben. Bei einer festen IP-Adresse wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Adresse ein.

Wichtiger Hinweis:

Falls Sie für diese Netzwerkkarte die Ausfallsicherung **Uplink Failover on Interace** konfigurieren möchten, beachten Sie bei der Eingabe des Netzwerks die Beschreibung zu dieser Funktion!

Default Gateway: Behalten Sie die Default-Einstellung **Assigned by remote** bei. Mögliche weitere Einstellungen sind **Static** und **None**.

Username: Tragen Sie hier den Benutzernamen ein, den Sie von Ihrem Provider erhalten haben.

Password: Tragen sie hier das Passwort ein, das Sie von Ihrem Provider erhalten haben.

Uplink Failover on Interface: Diese Funktion wird nur angezeigt, wenn im Drop-down-Menü **Default Gateway** die Einstellung **Assigned by remote** oder **Static** ausgewählt wurde.

Bei einer Schnittstelle zum Internet, können Sie mit Hilfe eines zweiten Internetzugangs und einer zusätzlichen Netzwerkkarte eine Ausfallsicherung einrichten. Beachten Sie dabei, dass das Internet-Sicherheitssystem nur eine DSL-Verbindung unterstützt. Eine Ausfallsicherung für den Internetzugang kann z. B. aus einer Standleitung und einem DSL-Zugang bestehen!

Bei einem Ausfall der primären Verbindung erfolgt dann automatisch der Uplink über den zweiten Internetzugang. Zur Überprüfung der Verbindung werden über die *primäre Netzwerkkarte* alle fünf Sekunden vier Ping-Anfragen an die **Uplink Failover check IP** gesendet. Erst wenn alle vier Ping-Anfragen nicht beantwortet werden, wird die Ersatznetzwerkkarte geladen.

Währenddem die Internetverbindung über die *Ersatznetzwerkkarte* (*Backup Interface*) erfolgt, werden die Ping-Anfragen weiter über die *primäre Netzwerkkarte* (*Primary Interface*) verschickt. Sobald das Sicherheitssystem wieder entsprechende Antwortpakete empfängt, erfolgt die Internetverbindung wieder über die *primäre Netzwerkkarte*.

Wichtiger Hinweis:

Für die Funktion **Uplink Failover on Interface** müssen auf der Primär- und auf der Ersatznetzwerkkarte zwei unterschiedliche Netzwerke definiert werden. Sie benötigen daher neben der zusätzlichen Netzwerkkarte für die Ersatzschnittstelle zwei separate Internetzugänge.

Per Default ist **Uplink Failover on Interface** ausgeschaltet (**Off**). Wenn diese Netzwerkkarte die primäre Verbindung zum Internet sein soll, stellen Sie im Drop-down-Menü **Primary Interface** ein. Falls diese Netzwerkkarte die Standby-Verbindung enthalten soll, wählen Sie die Einstellung **Backup Interface** aus.

Uplink Failover check IP: Dieses Eingabefeld wird angezeigt, wenn bei der Funktion **Uplink Failover on Interface** die Ein-

stellung **Primary Interface** ausgewählt ist. Geben Sie hier die IP-Adresse eines Hosts ein, der auf ICMP-Ping-Anfragen antwortet und zudem ständig erreichbar ist! Falls das System von dieser Adresse keine entsprechende Antwort erhält, wird durch die Ausfallsicherung die Backup-Schnittstelle aktiviert. In diesem Eingabefeld muss für die Ausfallsicherung immer eine IP-Adresse eingetragen sein!

QoS Status: Um auf einer Schnittstelle Bandbreitenmanagement mit der Funktion **Quality of Service (QoS)** durchzuführen, muss zuvor die Schnittstelle freigegeben und konfiguriert werden. Um die Schnittstelle für die Funktion **Quality of Service (QoS)** freizugeben, wählen Sie im Drop-down-Menü **On** aus.

Wichtiger Hinweis:

Für das Bandbreitenmanagement **Quality of Service (QoS)** müssen Sie die Werte **Uplink Bandwidth (kbits)** und **Downlink Bandwidth (kbits)** definieren. Die beiden Werte dienen als Rechengrundlage für das Bandbreitenmanagement. Falsche Angaben führen zu einem ungenauen Management der Datenströme. Die Funktion **Quality of Service (QoS)** wird in Kapitel 5.5.1 beschrieben.

Uplink Bandwidth (kbits): Diese Einstellung wird nur angezeigt, wenn die Funktion **QoS** eingeschaltet ist. In dieses Eingabemenü tragen Sie die für den Uplink verfügbare Bandbreite in vollen Kilobits ein. Diese ergibt sich aus den Werten der vorgeschalteten Schnittstelle oder Router. Bei einer Schnittstelle zum Internet ist es die Bandbreite der Internetverbindung - bei einem ADSL-Zugang beträgt die Uplink-Bandbreite z. B. 128 kBit/s, bei einer 2 Megabit Festverbindung z. B. 2048 kBit/s.

Downlink Bandwidth (kbits): Diese Einstellung wird nur angezeigt, wenn die Funktion **QoS** eingeschaltet ist. In dieses Eingabemenü tragen Sie die für den Downlink verfügbare Bandbreite in vollen Kilobits ein. Bei einer Schnittstelle zum Internet

ist es die Bandbreite der Internetverbindung - bei einem ADSL-Zugang beträgt die Downlink-Bandbreite z. B. 768 kBit/s, bei einer 2 Megabit Festverbindung z. B. 2048 kBit/s.

MTU Size: Die obere Grenze für die Größe der Datenpakete wird **MTU** bezeichnet. **MTU** steht für **Maximum Transfer Unit**. Bei Verbindungen die das Protokoll TCP/IP verwenden werden die Daten in Pakete aufgeteilt. Für diese Pakete wird eine maximale Größe bestimmt. Wenn nun diese obere Grenze zu hoch ist, kann es passieren, dass Datenpakete mit Informationen, die das Protokoll PPP over Ethernet betreffen, nicht richtig weitergeleitet und erkannt werden. Diese Datenpakete werden dann erneut verschickt. Allerdings kann die Performance auch eingeschränkt werden, wenn die obere Grenze zu niedrig definiert wird.

Beim Schnittstellen-Typ **PPP over Ethernet (PPPoE-DSL) Connection** ist per Default bereits ein MTU-Wert definiert: **1492** Byte.

6. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

Das System prüft nun die IP-Adresse und die Netzwerkmaske auf semantische Gültigkeit. Anschließend wird die neue Schnittstelle (**Interface**) in die Tabelle **Current Interface Status** geladen. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot)

7. Schalten Sie die Schnittstelle durch einen Klick auf die Statusampel ein.

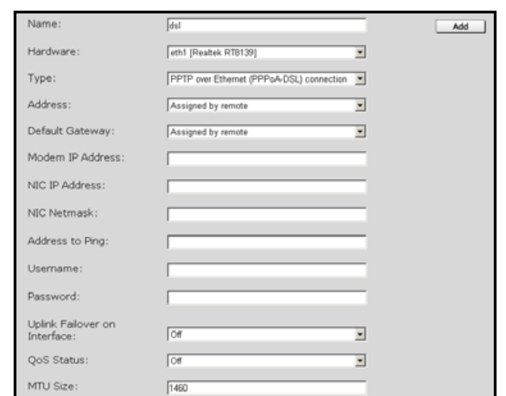
Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). In der Spalte **Oper** wird zu Beginn die Meldung **Down** angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu laden.

8. Laden Sie das Menü neu, indem Sie auf die Schaltläche **Refresh** klicken.

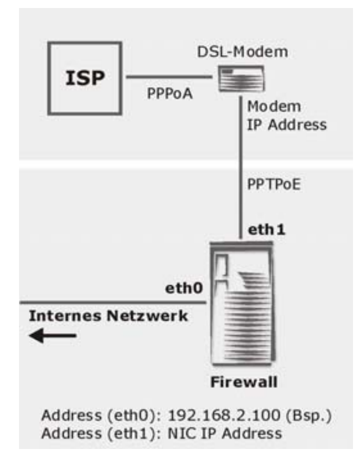
Weitere Informationen zur Funktion **Refresh** erhalten Sie in Kapitel 4.5 auf Seite 45.

Die neue Schnittstelle ist geladen, wenn die Meldung **Up** erscheint. Die Einstellungen werden in der Spalte **Parameters** angezeigt.

5.3.2.5. PPTPoE/PPPoA-DSL-Verbindung



Diesen Schnittstellen-Typ benötigen Sie, falls Sie eine **DSL**-Verbindung zum Internet mit dem Protokoll **PPP over ATM** aufbauen möchten. Zur konfiguration benötigen Sie auf dem Internet-Sicherheitssystem eine Ethernet-Netzwerkkarte und ein externes ADSL-Modem mit Ethernet-Anschluss. Die Verbindung zum Internet erfolgt über zwei Teilstrecken. Zwischen dem Internet-Sicherheitssystem und dem ADSL-Modem erfolgt die Verbindung mit dem Protokoll **PPTP over Ethernet**. Die Verbindung vom ADSL-Modem zum Internet Service Provider (ISP) erfolgt mit dem ADSL-Einwahlprotokoll **PPP over ATM** (siehe Grafik).



Für die Konfiguration benötigen Sie die DSL-Zugangsdaten inklusive Passwort. Die Daten erhalten Sie von Ihrem Provider.

Hinweis:

Die Installation und die nötigen Einstellungen am Internet-Sicherheitssystem speziell für den DSL-Zugang mit **AonSpeed** (Telekom Austria) wird im Leitfaden **Netzwerk mit AonSpeed** erklärt. Nachdem die Schnittstelle geladen wurde, ist das System 24 Stunden am Tag in das externe Netzwerk (Internet) eingewählt. Stellen Sie daher sicher, dass die Abrechnung bei ihrem Provider nach einem zeitunabhängigen Tarif erfolgt.
Sie finden den aktuellen Leitfaden unter der Internetadresse **http://www.astaro.com/kb**.

PPTP over Ethernet (PPPoA-DSL) einrichten:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Interfaces**.
2. Klicken Sie auf die Schaltfläche **New** um das Menü **Add Interface** zu öffnen.
3. Tragen Sie in das Eingabefeld **Name** den Namen der Schnittstelle ein.
4. Wählen Sie im Drop-down-Menü **Hardware** die Netzwerkkarte aus.

   Tipp:

   Wählen Sie als Schnittstelle zum externen Netzwerk (Internet) die Netzwerkkarte mit der Sys ID **eth1** aus.

   Eine Netzwerkkarte auf der bereits die primäre Netzwerkkarten-Adresse eingerichtet wurde, kann hier nicht mehr ausgewählt werden.

5. Wählen Sie im Drop-down-Menü **Type** den Schnittstellen-Typ **PPTP over Ethernet (PPPoA-DSL) connection** aus.

   Für diese Einstellungen benötigen Sie die Zugangsdaten für die DSL-Verbindung.

   Address: Behalten Sie die Default-Einstellung **Assigned by remote** bei, wenn Sie keine feste IP-Adresse haben.
   Bei einer festen IP-Adresse wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Adresse ein.

   ! **Wichtiger Hinweis:**

   Falls Sie für diese Netzwerkkarte die Ausfallsicherung **Uplink Failover on Interace** konfigurieren möchten, beachten Sie bei der Eingabe des Netzwerks die Beschreibung zu dieser Funktion!

   Default Gateway: Behalten Sie die Default-Einstellung **Assigned by remote** bei. Mögliche weitere Einstellungen sind **Static** und **None**.

   Modem IP Address: Tragen Sie hier die IP-Adresse des ADSL-Modems ein. Diese Adresse wird in der Regel vom Provider oder von der Hardware mitgeliefert und kann nicht geändert werden.
   Beispiel: 10.0.0.138 (bei **AonSpeed**)

   NIC IP Address: Tragen Sie hier die IP-Adresse für die Netzwerkkarte auf dem Internet-Sicherheitssystem ein. Die Adresse muss im selben Sub-Netzwerk liegen wie die IP-Adresse des Modems.
   Beispiel: 10.0.0.140 (bei **AonSpeed**)

   NIC Netmask: Tragen Sie hier die Netzwerkmaske ein.
   Beispiel: 255.255.255.0 (bei **AonSpeed**)

   Address to Ping: Geben Sie hier die IP-Adresse eines Hosts im Internet ein, der auf ICMP-Ping-Anfragen antwortet (z. B. der DNS-Server Ihres Internet Service Providers). Falls das System von dieser Adresse keine entsprechende Antwort erhält, wird der Verbindungsaufbau abgebrochen.

Username: Tragen Sie hier den Benutzernamen ein, den Sie von Ihrem Provider erhalten haben.

Password: Tragen sie hier das Passwort ein, das Sie von Ihrem Provider erhalten haben.

Uplink Failover on Interface: Diese Funktion wird nur angezeigt, wenn im Drop-down-Menü **Default Gateway** die Einstellung **Assigned by remote** oder **Static** ausgewählt wurde.

Bei einer Schnittstelle zum Internet, können Sie mit Hilfe eines zweiten Internetzugangs und einer zusätzlichen Netzwerkkarte eine Ausfallsicherung einrichten. Beachten Sie dabei, dass das Internet-Sicherheitssystem nur eine DSL-Verbindung unterstützt. Eine Ausfallsicherung für den Internetzugang kann z. B. aus einer Standleitung und einem DSL-Zugang bestehen!

Bei einem Ausfall der primären Verbindung erfolgt dann automatisch der Uplink über den zweiten Internetzugang. Zur Überprüfung der Verbindung werden über die *primäre Netzwerkkarte* alle fünf Sekunden vier Ping-Anfragen an die **Uplink Failover check IP** gesendet. Erst wenn alle vier Ping-Anfragen nicht beantwortet werden, wird die Ersatznetzwerkkarte geladen.

Währenddem die Internetverbindung über die *Ersatznetzwerkkarte* (*Backup Interface*) erfolgt, werden die Ping-Anfragen weiter über die *primäre Netzwerkkarte* (*Primary Interface*) verschickt. Sobald das Sicherheitssystem wieder entsprechende Antwortpakete empfängt, erfolgt die Internetverbindung wieder über die *primäre Netzwerkkarte*.

Wichtiger Hinweis:

Für die Funktion **Uplink Failover on Interface** müssen auf der Primär- und auf der Ersatznetzwerkkarte zwei unterschiedliche Netzwerke definiert werden. Sie benötigen daher neben der zusätzlichen Netzwerkkarte für die Ersatzschnittstelle zwei separate Internetzugänge.

Per Default ist **Uplink Failover on Interface** ausgeschaltet (**Off**). Wenn diese Netzwerkkarte die primäre Verbindung zum Internet sein soll, stellen Sie im Drop-down-Menü **Primary Interface** ein. Falls diese Netzwerkkarte die Standby-Verbindung enthalten soll, wählen Sie die Einstellung **Backup Interface** aus.

Uplink Failover check IP: Dieses Eingabefeld wird angezeigt, wenn bei der Funktion **Uplink Failover on Interface** die Einstellung **Primary Interface** ausgewählt ist. Geben Sie hier die IP-Adresse eines Hosts ein, der auf ICMP-Ping-Anfragen antwortet (z. B. der DNS-Server Ihres Internet Service Providers). Falls das System von dieser Adresse keine entsprechende Antwort erhält, wird durch die Ausfallsicherung die Backup-Schnittstelle aktiviert. In diesem Eingabefeld muss für die Ausfallsicherung immer eine IP-Adresse eingetragen sein.

QoS Status: Um auf einer Schnittstelle Bandbreitenmanagement mit der Funktion **Quality of Service (QoS)** durchzuführen, muss zuvor die Schnittstelle freigegeben und konfiguriert werden. Um die Schnittstelle für die Funktion **Quality of Service (QoS)** freizugeben, wählen Sie im Drop-down-Menü **On** aus.

Wichtiger Hinweis:

Für das Bandbreitenmanagement **Quality of Service (QoS)** müssen Sie die Werte **Uplink Bandwidth (kbits)** und **Downlink Bandwidth (kbits)** definieren. Die beiden Werte dienen als Rechengrundlage für das Bandbreitenmanagement. Falsche Angaben führen zu einem ungenauen Management der Datenströme. Die Funktion **Quality of Service (QoS)** wird in Kapitel 5.5.1 beschrieben.

Uplink Bandwidth (kbits): Diese Einstellung wird nur angezeigt, wenn die Funktion **QoS** eingeschaltet ist. In dieses Eingabemenü tragen Sie die für den Uplink verfügbare Bandbreite in vollen Kilobits ein. Diese ergibt sich aus den Werten der

vorgeschalteten Schnittstelle oder Router. Bei einer Schnittstelle zum Internet ist es die Bandbreite der Internetverbindung - bei einem ADSL-Zugang beträgt die Uplink-Bandbreite z. B. 128 kBit/s, bei einer 2 Megabit Festverbindung z. B. 2048 kBit/s.

Downlink Bandwidth (kbits): Diese Einstellung wird nur angezeigt, wenn die Funktion **QoS** eingeschaltet ist. In dieses Eingabemenü tragen Sie die für den Downlink verfügbare Bandbreite in vollen Kilobits ein. Bei einer Schnittstelle zum Internet ist es die Bandbreite der Internetverbindung - bei einem ADSL-Zugang beträgt die Downlink-Bandbreite z. B. 768 kBit/s, bei einer 2 Megabit Festverbindung z. B. 2048 kBit/s.

MTU Size: Die obere Grenze für die Größe der Datenpakete wird **MTU** bezeichnet. **MTU** steht für **Maximum Transfer Unit**. Bei Verbindungen die das Protokoll TCP/IP verwenden werden die Daten in Pakete aufgeteilt. Für diese Pakete wird eine maximale Größe bestimmt. Wenn nun diese obere Grenze zu hoch ist, kann es passieren, dass Datenpakete mit Informationen, die das Protokoll PPP over Ethernet betreffen, nicht richtig weitergeleitet und erkannt werden. Diese Datenpakete werden dann erneut verschickt. Allerdings kann die Performance auch eingeschränkt werden, wenn die obere Grenze zu niedrig definiert wird.
Im Eingabefeld **MTU Size** muss beim Schnittstellen-Typ **PPP over Ethernet (PPPoA-DSL) Connection** ein Wert für die maximale Übertragungsrate in Bytes definiert werden.

Beim Schnittstellen-Typ **PPP over Ethernet (PPPoA-DSL) Connection** ist per Default bereits ein MTU-Wert definiert: **1460** Byte.

6. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

Das System prüft nun die IP-Adresse und die Netzwerkmaske auf semantische Gültigkeit. Anschließend wird die neue Schnittstelle (**Interface**) in die Tabelle **Current Interface Status** geladen. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot)

7. Schalten Sie die Schnittstelle durch einen Klick auf die Statusampel ein.

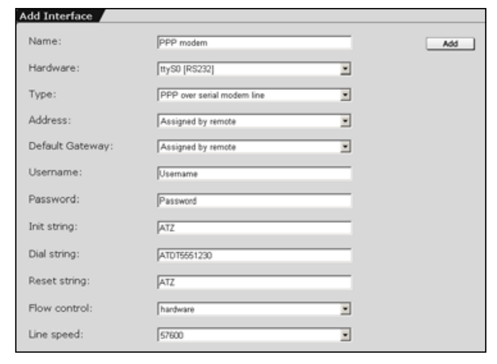
   Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). In der Spalte **Oper** wird zu Beginn die Meldung **Down** angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu laden.

8. Laden Sie das Menü neu, indem Sie auf die Schaltläche **Refresh** klicken.

   Weitere Informationen zur Funktion **Refresh** erhalten Sie in Kapitel 4.5 auf Seite 45.

Die neue Schnittstelle ist geladen, wenn die Meldung **Up** erscheint. Die Einstellungen werden in der Spalte **Parameters** angezeigt.

5.3.2.6. PPP over Serial Modem Line



Diesen Schnittstellen-Typ benötigen Sie, falls Sie eine Verbindung zum Internet mit einem **PPP**-Modem über die serielle Schnittstelle aufbauen möchten. Zur konfiguration benötigen Sie auf dem Internet-Sicherheitssystem eine serielle Schnittstelle und ein externes PPP-Modem.

Für die Konfiguration benötigen Sie die DSL-Zugangsdaten inklusive Passwort. Die Daten erhalten Sie von Ihrem Provider.

PPP over Serial Modem einrichten:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Interfaces**.

2. Klicken Sie auf die Schaltfläche **New** um das Menü **Add Interface** zu öffnen.

3. Tragen Sie in das Eingabefeld **Name** den Namen der Schnittstelle ein.

4. Wählen Sie im Drop-down-Menü **Hardware** die serielle Schnittstelle aus.

5. Wählen Sie im Drop-down-Menü **Type** den Schnittstellen-Typ **PPP over serial modem line** aus.

   Address: Behalten Sie die Default-Einstellung **Assigned by remote** bei, wenn Sie keine feste IP-Adresse haben.
   Bei einer festen IP-Adresse wählen Sie im Drop-down-Menü **Static** aus und tragen in das Eingabefeld die Adresse ein.

   Wichtiger Hinweis:

   Falls Sie für diese Netzwerkkarte die Ausfallsicherung **Uplink Failover on Interace** konfigurieren möchten, beachten Sie bei der Eingabe des Netzwerks die Beschreibung zu dieser Funktion!

   Default Gateway: Behalten Sie die Default-Einstellung **Assigned by remote** bei. Mögliche weitere Einstellungen sind **Static** und **None**.

   Username: Tragen Sie hier den Benutzernamen ein, den Sie von Ihrem Provider erhalten haben.

   Password: Tragen Sie hier das Passwort ein, das Sie von Ihrem Provider erhalten haben.

   Init String: Tragen Sie in das Einagbefeld den String zur Initialisierung des Modems ein. Beachten Sie, dass der *Init String* eventuell dem Modem angepasst werden muss. In diesem Fall entnehmen Sie den *Init String* dem zugehörigen Modem-Handbuch. Falls Sie keine entsprechende Dokumentation zur Verfügung haben, tragen Sie in das Eingabefeld **ATZ** ein.

   Dial String: Tragen Sie in das Eingabefeld **ATDT** gefolgt von der Telefonnumer ein. **Beispiel**: ATDT5551230

Reset String: Tragen Sie in das Einagbefeld den *Reset String* für das Modem ein. Beachten Sie auch hier, dass der *Reset String* eventuell dem Modem angepasst werden muss. In diesem Fall entnehmen Sie diesen dem zugehörigen Modem-Handbuch. Falls Sie keine entsprechende Dokumentation zur Verfügung haben, tragen Sie in das Eingabefeld ebenfalls **ATZ** ein.

Flow Control: Diese Funktion dient zur Kontrolle des Datenflusses. Wenn die Daten über die serielle Verbindung laufen, kann es vorkommen, dass das System die ankommenden Daten nicht schnell genug verarbeiten kann. Um sicherzustellen, dass keine Daten verloren gehen, ist eine Methode zur Kontrolle des Datenflusses notwendig.
Bei der seriellen Verbindung stehen zwei Methoden zur Auswahl:

- **Hardware-Signale**
- **Software-Signale**

Da bei einer PPP-Verbindung alle 8 Bits der Leitung verwendet werden, und sich in den übertragenen Daten die Bytes der Steuerzeichen *Control S* und *Control Q* befinden, empfehlen wir, die Default-Einstellung **Hardware** beizubehalten und ein entsprechendes serielles Verbindungskabel zu verwenden.

Line Speed: Stellen Sie hier die Geschwindigkeit in Bits pro Sekunde für die Verbindung zwischen dem Sicherheitssystem und dem Modem ein.
Übliche Werte sind 57600 Bits/s und 115200 Bits/s.

Uplink Failover on Interface: Diese Funktion wird nur angezeigt, wenn im Drop-down-Menü **Default Gateway** die Einstellung **Assigned by remote** oder **Static** ausgewählt wurde.

Bei einer Schnittstelle zum Internet, können Sie mit Hilfe eines zweiten Internetzugangs, z. B. über die serielle Schnittstelle und einem PPP-Modem eine Ausfallsicherung einrichten.
Eine Ausfallsicherung für den Internetzugang kann z. B. aus einer Standleitung und einem Zugang über die serielle Schnittstelle bestehen! Bei einem Ausfall der primären Verbindung er-

folgt dann automatisch der Uplink über den zweiten Internetzugang. Zur Überprüfung der Verbindung werden über die *primäre Netzwerkkarte* alle fünf Sekunden vier Ping-Anfragen an die **Uplink Failover check IP** gesendet. Erst wenn alle vier Ping-Anfragen nicht beantwortet werden, wird die Ersatzschnittstelle geladen.

Währenddem die Internetverbindung über die *Ersatzschittstelle* (*Backup Interface*) erfolgt, werden die Ping-Anfragen weiter über die *primäre Netzwerkkarte* (*Primary Interface*) verschickt. Sobald das Sicherheitssystem wieder entsprechende Antwortpakete empfängt, erfolgt die Internetverbindung wieder über die *primäre Netzwerkkarte*.

Wichtiger Hinweis:

Für die Funktion **Uplink Failover on Interface** müssen auf der Primär- und auf der Ersatzschnittstelle zwei unterschiedliche Netzwerke definiert werden. Sie benötigen daher neben der zusätzlichen Netzwerkkarte für die Ersatzschnittstelle zwei separate Internetzugänge.

Per Default ist **Uplink Failover on Interface** ausgeschaltet (**Off**). Wenn diese Schnittstelle die primäre Verbindung zum Internet sein soll, stellen Sie im Drop-down-Menü **Primary Interface** ein. Falls diese Schnittstelle die Standby-Verbindung enthalten soll, wählen Sie die Einstellung **Backup Interface** aus.

Uplink Failover check IP: Dieses Eingabefeld wird angezeigt, wenn bei der Funktion **Uplink Failover on Interface** die Einstellung **Primary Interface** ausgewählt ist. Geben Sie hier die IP-Adresse eines Hosts ein, der auf ICMP-Ping-Anfragen antwortet (z. B. der DNS-Server Ihres Internet Service Providers). Falls das System von dieser Adresse keine entsprechende Antwort erhält, wird durch die Ausfallsicherung die Backup-Schnittstelle aktiviert. In diesem Eingabefeld muss für die Ausfallsicherung immer eine IP-Adresse eingetragen sein.

QoS Status: Um auf einer Schnittstelle Bandbreitenmanagement mit der Funktion **Quality of Service (QoS)** durchzuführen, muss zuvor die Schnittstelle freigegeben und konfiguriert werden. Um die Schnittstelle für die Funktion **Quality of Service (QoS)** freizugeben, wählen Sie im Drop-down-Menü **On** aus.

Wichtiger Hinweis:

Für das Bandbreitenmanagement **Quality of Service (QoS)** müssen Sie die Werte **Uplink Bandwidth (kbits)** und **Downlink Bandwidth (kbits)** definieren. Die beiden Werte dienen als Rechengrundlage für das Bandbreitenmanagement. Falsche Angaben führen zu einem ungenauen Management der Datenströme. Die Funktion **Quality of Service (QoS)** wird in Kapitel 5.5.1 beschrieben.

Uplink Bandwidth (kbits): Diese Einstellung wird nur angezeigt, wenn die Funktion **QoS** eingeschaltet ist. In dieses Eingabemenü tragen Sie die für den Uplink verfügbare Bandbreite in vollen Kilobits ein. Diese ergibt sich aus den Werten der vorgeschalteten Schnittstelle oder Router. Bei einer Schnittstelle zum Internet ist es die Bandbreite der Internetverbindung.

Downlink Bandwidth (kbits): Diese Einstellung wird nur angezeigt, wenn die Funktion **QoS** eingeschaltet ist. In dieses Eingabemenü tragen Sie die für den Downlink verfügbare Bandbreite in vollen Kilobits ein. Bei einer Schnittstelle zum Internet ist es die Bandbreite der Internetverbindung.

MTU Size: Die obere Grenze für die Größe der Datenpakete wird **MTU** bezeichnet. **MTU** steht für **Maximum Transfer Unit**. Bei Verbindungen die das Protokoll TCP/IP verwenden werden die Daten in Pakete aufgeteilt. Für diese Pakete wird eine maximale Größe bestimmt. Wenn nun diese obere Grenze zu hoch ist, kann es passieren, dass Datenpakete mit Informationen, die das Protokoll PPP over Ethernet betreffen, nicht richtig weitergeleitet und erkannt werden. Diese Datenpakete werden dann erneut

verschickt. Allerdings kann die Performance auch eingeschränkt werden, wenn die obere Grenze zu niedrig definiert wird.

Im Eingabefeld **MTU Size** muss beim Schnittstellen-Typ **PPP over Ethernet (PPPoA-DSL) Connection** ein Wert für die maximale Übertragungsrate in Bytes definiert werden.

Beim Schnittstellen-Typ **PPP over Ethernet (PPPoA-DSL) Connection** ist per Default bereits ein MTU-Wert definiert: **1460** Byte.

6. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

   Das System prüft nun die IP-Adresse und die Netzwerkmaske auf semantische Gültigkeit. Anschließend wird die neue Schnittstelle (**Interface**) in die Tabelle **Current Interface Status** geladen. Die Schnittstelle ist noch ausgeschaltet (Statusampel zeigt Rot)

7. Schalten Sie die Schnittstelle durch einen Klick auf die Statusampel ein.

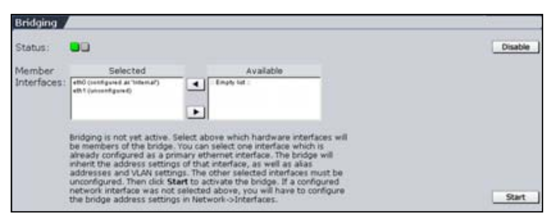
   Die Schnittstelle ist nun eingeschaltet (Statusampel zeigt Grün). In der Spalte **Oper** wird zu Beginn die Meldung **Down** angezeigt. Das System benötigt kurze Zeit, um die neue Schnittstelle zu laden.

8. Laden Sie das Menü neu, indem Sie auf die Schaltläche **Refresh** klicken.

   Weitere Informationen zur Funktion **Refresh** erhalten Sie in Kapitel 4.5 auf Seite 45.

Die neue Schnittstelle ist geladen, wenn die Meldung **Up** erscheint. Die Einstellungen werden in der Spalte **Parameters** angezeigt.

5.3.3. Bridging



Durch das **Bridging** können zwei oder auch mehrere gleichartige Ethernet-Netzwerke oder – Netzwerksegmente miteinander verbunden werden. Die Datenpakete werden mittels Bridging-Tabellen weitergeleitet, die MAC-Adressen einem Bridge Port zuordnen. Die *Bridge* arbeitet auf Schicht 2 des ISO/OSI-Schichten-Modells (siehe dazu Kapitel 2 ab Seite 11) der offenen Kommunikation und ist von höheren Protokollen unabhängig.

Bei diesem Sicherheitssysten werden die beteiligten Netzwerke durch die Auswahl der zugehörigen Netzwerkarten definiert. Die resultierende *Bridge* wird im Menü **Interfaces** in der Tabelle **Hardware List** als eine Netzwerkkarte mit der *Sys ID* **br0** angezeigt. Obwohl der Datenverkehr transparent über die an der *Bridge* beteiligten Netzwerkkarten geführt wird, muss dieser durch entsprechende Paketfilterregeln explizit erlaubt werden. Die Paketfilterregeln werden im Menü **Packet Filter/Rules** gesetzt.

Bridging definieren:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Bridging**.

2. Schalten Sie die Funktion durch einen Klick auf die Schaltfläche **Enable** ein.

   Die Statusampel zeigt Grün.

3. Wählen Sie im Auswahlfeld **Member Interfaces** die Netzwerkkarten zu den entsprechenden Netzwerken aus.

   Wählen Sie mindestens zwei Netzwerkkarten aus. Für das Bridging kann nur eine bereits konfigurierte Netzwerkkarte ausgewählt werden. Die Bridge wird anschließend alle auf dieser

Netzwerkkarte definierten Adressen, wie z. B. *Additional Addresses* oder *VLAN*-Einstellungen übernehmen.

Falls Sie für das *Bridging* nur unkonfigurierte Netzwerkkarten ausgewählt haben, können Sie die Definition der IP-Adressen auch nachträglich im Menü **Network/Interfaces** durchführen.

4. Starten Sie die Funktion durch einen Klick auf die Schaltfläche **Start**.

Die Netzwerkkarten werden nun miteinander verbunden und die *Bridge* wird aktiviert. Die ausgewählten Netzwerkkarten werden in der Tabelle **Current Bridged Interfaces** angezeigt. Anschließend stehen Ihnen in dieser Tabelle weitere Funktionen zur Verfügung.

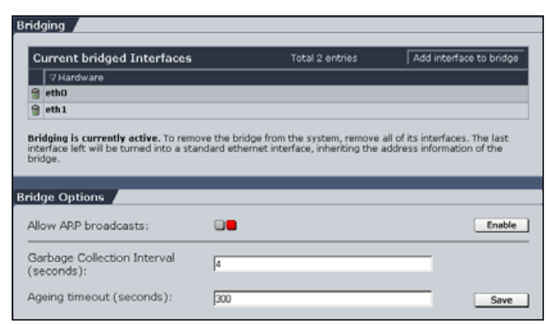
Weitere Funktionen

Netzwerkkarte hinzufügen: Durch einen Klick auf die Schaltfläche **Add interface to Bridge** wird eine neue Zeile in die Tabelle importiert. Mit einem Klick auf die Meldung **Click here to select interface** wird ein Auswahlfeld geöffnet. Wählen Sie nun die neue Netzwerkkarte aus und speichern Sie die Einstellung durch einen Klick auf die Schaltfläche **Save**. Mit der Schaltfläche **Cancel** wird die Auswahl wieder verworfen.

Netzwerkkarte löschen: Durch einen Klick auf das Papierkorb-Symbol wird die Netzwerkkarte aus der Tabelle gelöscht. Wenn Sie die Bridge deaktivieren möchten, löschen Sie nacheinander die Einträge bis nur noch eine Netzwerkkarte übrig ist. Diese Netzwerkkarte wird anschließend in ein *Standard Ethernet Interface* geändert und übernimmt alle Adress-Einstellungen von der *Bridge*.

Bridge Options

Dieses Fenster wird angezeigt, wenn eine Bridge in Betrieb ist.



Allow ARP broadcasts: Mit dieser Funktion können Sie bestimmen, ob eingehende **ARP Broadcasts** von der *Bridge* weitergeleitet werden. Im eingeschalteten Zustand erlaubt die *Bridge* Anfragen an die MAC-Zieladresse FF:FF:FF:FF:FF:FF. Dies kann eventuell von mutmaßlichen Angreifern genutzt werden, um Informationen über die Netzwerkarten im entsprechenden Netzwerksegment oder sogar auf dem Sicherheitssystem selbst zu sammeln. Falls derartige Anfragen die Bridge passieren, sollte diese Funktion daher ausgeschaltet werden. Im voreingestellten Zustand ist die Funktion Allow ARP Broadcasts eingeschaltet (Statusampel zeigt grün).

Das Modul entfernt nach einer bestimmten Zeitspanne inaktive MAC-Adressen aus der Bridging-Tabelle.

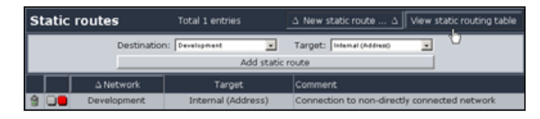
Garbage Collection Intervall (**seconds**): In diesem Eingabefeld stellen Sie ein, in welchem Zeitintervall die Bridging-Tabelle nach inaktiven MAC-Adressen durchsucht wird. Adressen mit entsprechender Zeitüberschreitung werden gelöscht. Die Funktion ist auf 4 Sekunden voreingestellt.

Ageing timeout: In diesem Eingabefeld stellen Sie ein, nach welcher Zeitspanne eine inaktive Adresse gelöscht wird. Die Funktion ist auf 300 Sekunden voreingestellt.

5.3.4. Routing

Jeder an ein Netzwerk angeschlossene Rechner verwendet eine Routing-Tabelle. Mittels dieser Routing-Tabelle stellt der Rechner fest, ob er ein Datenpaket direkt an den Zielrechner im gleichen Netzwerk oder an einen Router versenden muss.

Static Routes



Für die direkt angeschlossenen Netzwerke trägt das Internet-Sicherheitssystem die entsprechenden Routing-Einträge selbst ein. Weitere Einträge müssen manuell vorgenommen werden. Dies ist z. B. der Fall, wenn im lokalen Netzwerk ein weiterer Router existiert, über den ein bestimmtes Netzwerk erreicht werden soll.

Routen für Netzwerke, die nicht direkt angeschlossen sind, aber über einen Befehl oder eine Konfigurationsdatei in die Routing-Tabelle eingetragen werden, bezeichnet man als statische Routen.

In diesem Menü können Sie festlegen, welches Netzwerk zu welcher Netzwerkkarte oder zu welcher externen IP-Adresse geroutet wird.

Statische Routes definieren:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Routing**.
2. Klicken Sie auf die Schaltfläche **New static route**.

   Ein erweitertes Eingabemenü wird geöffnet.
3. Wählen Sie im Drop-down-Menü **Destination** das Netzwerk aus. Im Drop-down-Menü **Destination** sind alle statischen sowie die in den Menüs **Networks** und **Interfaces** neu definierten Netzwerke enthalten.

4. Wählen Sie im Drop-down-Menü **Target** das Ziel aus.
   Namen in zwei spitzen Klammern kennzeichnen Netzwerkkarten (**Interfaces**). Bei Namen ohne Klammern handelt es sich um einen Host oder um einen Router.

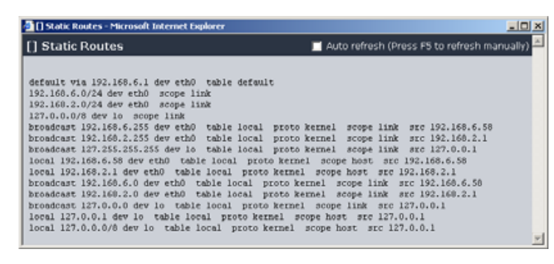
5. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add static route**.

   Nach erfolgreicher Definition wird die neue **Static Route** immer deaktiviert in die Static-Route-Tabelle eingetragen (Statusampel zeigt Rot).

6. Aktivieren Sie die statische Route durch einen Klick auf die Statusampel.

Durch einen Klick auf das Papierkorb-Symbol wird der Eintrag wieder gelöscht.

Kernel Routing Table



Die **Kernel-Routing**-Tabelle wird in einem separaten Fenster dargestellt. In diesem Fenster werden alle vom System aktuell verwendeten Routen aufgelistet. Das System arbeitet die Routen in der dargestellten Reihenfolge ab. Die erste zutreffende Route wird verwendet. Per Default sind die Routen der Netzwerkkarten bereits eingetragen und nicht editierbar.

Durch einen Klick auf die Schaltfläche **View static routing table** wird das Fenster geöffnet.

Policy Routes

Das Policy-basierte Routing ermöglicht die Weiterleitung bzw. das Routen von Datenpaketen nach eigenen sicherheitspolischen Richtlinien. Durch die erweiterten Einstellungen kann der Datenverkehr auf mehrere Internet-Uplinks verteilt werden. Dies ermöglicht Ihnen u.a. Kosten einzusparen sowie den Einfluss auf die genutzte Bandbreite und die Prioritäten.

Policy Routes definieren:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Routing**.
2. Klicken Sie im Fenster Policy Routes auf die Schaltfläche **New policy route**.

   Anschließend wird das Eingabefenster geöffnet.
3. Führen Sie die folgenden Einstellungen durch:

   Position: Bestimmen Sie, in welche Zeile der Tabelle die Route eingefügt werden soll. Die Reihenfolge der Route kann auch später geändert werden. Per Default wird die Route an das Ende (**To Bottom**) der Route-Tabelle eingefügt.

   Source: Wählen Sie im Drop-down-Menü das Quellnetzwerk der Datenpakete aus, die geroutet werden sollen. Die Einstellung **Any** trifft auf alle Netzwerke zu.

   Destination: Wählen Sie im Drop-down-Menü das Zielnetzwerk der Datenpakete aus. Die Einstellung **Any** trifft auf alle Netzwerke zu.

   Service: Wählen Sie im Drop-down-Menü den Dienst aus.

   Im Drop-down-Menü sind sowohl die vordefinierten als auch die von Ihnen selbst festgelegten Dienste enthalten. Mit Hilfe dieser Dienste lässt sich der zu bearbeitende Datenverkehr präzise definieren. Die Einstellung **Any** steht hier stellvertretend für alle Kombinationen aus Protokollen und Quell- bzw. Zielport.

Source Interface: Wählen Sie hier für die auf dem Sicherheitssystem eingehenden Datenpakete, die anschließend geroutet werden, eine Netzwerkkarte aus.

Target: Wählen Sie in diesem Drop-down-Menü die Ziel-IP-Adresse für die Datenpakete aus.
Als Ziel kann entweder eine Netwerkkarte auf dem Sicherheitssystem oder ein „Next-Hop“-Host eingestellt werden.

4. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add static route**.

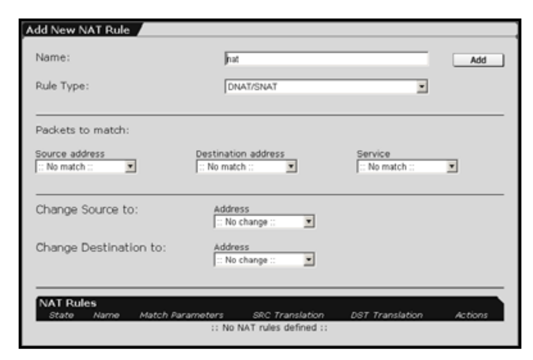
   Nach erfolgreicher Definition wird die neue **Static Route** immer deaktiviert in die Static-Route-Tabelle eingetragen (Statusampel zeigt Rot).

5. Aktivieren Sie die statische Route durch einen Klick auf die Statusampel.

Durch einen Klick auf das Papierkorb-Symbol wird der Eintrag wieder gelöscht.

5.3.5. NAT/Masquerading

5.3.5.1. NAT



Die Funktion **Network Address Translation (NAT)** dient zur Umsetzung der - meist privaten - IP-Adressen eines Netzwerkes auf andere - meist öffentliche - IP-Adressen eines anderen Netzwerkes. NAT ermöglicht damit mehreren PCs in einem LAN, einerseits die IP-Adresse des Internet-Access-Routers für den Internet-Zugang zu nutzen, und andererseits versteckt es das LAN hinter der im Internet registrierten IP-Adresse des Routers.

Wenn ein Client im LAN ein IP-Paket an den Router schickt, wandelt NAT die Adresse des Absenders in eine gültige IP-Adresse um (die ihm etwa der Provider zugeteilt hat), bevor es ins Internet weitergereicht wird. Kommt von der entfernten Station eine Antwort auf dieses Paket zurück, wandelt NAT die Empfängeradresse wieder in die ursprüngliche IP-Adresse der lokalen Station um und stellt das Paket ordnungsgemäß zu. Theoretisch kann NAT interne Netzwerke (LANs) mit beliebig vielen Clients verwalten.

Durch **Destination Network Address Translation (DNAT)** wird die Zieladresse (**Destination Address**) der IP-Pakete umgeschrieben. Dies ist besonders interessant, wenn Sie ein privates Netzwerk hinter Ihrem Internet-Sicherheitssystem betreiben und Netzwerkdienste im Internet verfügbar machen wollen.

Wichtiger Hinweis:

DNAT kann nicht in Verbindung mit **PPTP VPN Access** verwendet werden.

Beispiel:

Ihr internes Netzwerk hat den Addressraum 192.168.0.0/255.255.255.0. Sie möchten nun Ihren Webserver, der auf dem Server mit der IP-Addresse 192.168.0.20 auf Port 80 läuft, für Clients aus dem Internet erreichbar machen.
Die Clients können dessen Adresse nicht direkt ansprechen, da der Adressbereich 192.168 im Internet nicht geroutet wird. Es ist jedoch möglich, vom Internet aus die externe Addresse Ihres Internet-Sicherheitssystems anzusprechen. Mit **DNAT** können Sie z. B. den Port 80 auf der externen Schnittstelle des Internet-Sicherheitssystems auf den Webserver umleiten.

Hinweis:

Die Einstellungen für einen Webserver hinter dem Internet-Sicherheitssystem werden im Leitfaden **Web Server/DNAT** beschrieben. Sie finden den aktuellen Leitfaden unter der Internetadresse **http://www.astaro.com/kb**.

Die Funktionalität von **Source Network Address Translation (SNAT)** entspricht der von **DNAT**, mit dem Unterschied, dass statt der Zieladresse (**Destination Address**) der IP-Pakete die Quelladresse (**Source Address**) umgeschrieben wird.
Dies kann in komplexen Netzwerken nützlich sein, um Antworten auf Verbindungen in andere Netzwerke oder auf andere Hosts umzuleiten.

Tipp:

Um eine einfache Anbindung von privaten Netzwerken an das externe Netzwerk (Internet) zu erreichen, sollten Sie anstatt **SNAT** die Funktion **Masquerading** verwenden.

Im Gegensatz zum (dynamischen) **Masquerading** handelt es sich bei **SNAT** um eine statische Adressumsetzung, d. h. jeder internen IP-Adresse wird genau eine extern sichtbare **IP-Adresse** zugewiesen.

Hinweis:

Um den Port 443 (HTTPS) umzuleiten, müssen Sie im Menü **System / WebAdmin Settings** den **WebAdmin TCP Port** auf einen anderen Wert ändern (z. B. 1443). Diese Funktion wird in Kapitel 5.1.9 im Abschnitt **General Settings** beschrieben.

Hinweis:

Da die Adressumsetzung vor der Filterung durch **Paketfilterregeln** erfolgt, müssen Sie im Menü **Packet Filter / Rules** die entsprechenden Regeln setzen. Das Setzen der Paketfilterregeln wird ausführlich in Kapitel 5.4 ab Seite 223 beschrieben.

NAT-Regel setzen:

1. Öffnen Sie im Verzeichnis **Network** das Menü **NAT / Masquerading**.

2. Vergeben Sie im Eingabefeld **Name** einen eindeutigen Namen für die **NAT-Regel**.

3. Wählen Sie im Drop-down-Menü **Rule Type** die Funktion **DNAT / SNAT** aus.

   Anschließend öffnet sich ein erweitertes Eingabefenster.

4. Definieren Sie im Fenster **Packets to match** welche Pakete zu einer neuen Adresse umgeleitet bzw. in einen anderen Dienst übersetzt werden sollen.

   Damit eine gültige DNAT/SNAT-Regel definiert werden kann, muss in diesem Fenster mindestens ein Parameter ausgewählt werden. Die Einstellung **No match** hat zur Folge, dass zwischen den Parametern in dieser Auswahl nicht unterschieden wird.

   Source Address: Wählen Sie die original Quelladresse aus. Es kann ein Host oder ein gesamtes Netzwerk ausgewählt werden.

Destination Address: Wählen Sie die original Zieladresse aus. Es kann ein Host oder ein gesamtes Netzwerk ausgewählt werden.

Service: Wählen Sie den original Dienst aus. Dieser Dienst besteht aus Quell- und Zielport der Pakete oder einem Protokoll, z. B. TCP.

Hinweis:

Ein **Dienst** (**Service**) kann nur umgeleitet werden, wenn auch die kommunizierenden Adressen umgeleitet werden. Des Weiteren kann ein Dienst nur in einen Dienst mit gleichem Protokoll übersetzt werden.

---

5. Definieren Sie mit den folgenden Drop-down-Menüs wohin die Pakete umgeleitet werden sollen.

   Damit eine gültige DNAT/SNAT-Regel definiert werden kann, muss in diesem Fenster mindestens ein Parameter ausgewählt werden. Wenn Sie die original Adresse auf ein gesamtes Netzwerk umleiten, werden die darin enthaltenen IP-Adressen der Reihe nach ausgewählt.

   Change Source to *(SNAT)*: Wählen Sie die neue Quelladresse für die IP-Pakete aus. Es kann nur eine Schnittstelle ausgewählt werden.

   Service Source: Dieses Drop-down-Menü wird angezeigt, wenn Sie bei **Change source to** eine Adresse ausgewählt haben. Es können hier nur Dienste (Services) mit einem Quellport ausgewählt werden.

   Change Destination to *(DNAT)*: Wählen Sie die neue Zieladresse für die IP-Pakete aus. Es kann ein Host oder ein gesamtes Netzwerk ausgewählt werden.

   Service Destination: Dieses Drop-down-Menü wird angezeigt, wenn Sie bei **Change Destination to** eine Adresse auswählen.

6. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

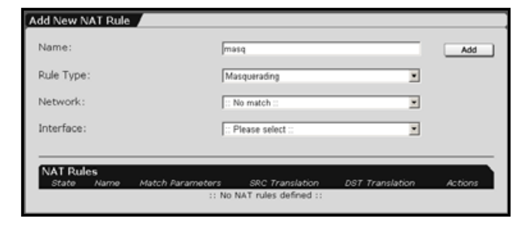
Nach erfolgreicher Definition wird die neue DNAT/SNAT-Regel in die Tabelle **NAT Rules** übernommen. Anschließend stehen Ihnen in der NAT-Tabelle weitere Funktionen zur Verfügung.

Weitere Funktionen

Einträge editieren: Durch einen Klick auf die Schaltfläche **edit** wird die Regel in das Fenster **Edit NAT Rule** geladen. Anschließend können Sie die Eingaben bearbeiten.

Einträge löschen: Durch einen Klick auf die Schaltfläche **delete** wird der Eintrag aus der Tabelle gelöscht.

5.3.5.2. Masquerading



Masquerading ist eine Sonderform von **SNAT**, bei der viele private IP-Adressen auf eine einzige öffentliche IP-Adresse umgesetzt werden, d. h. Sie verbergen interne IP-Adressen und Netzwerkinformationen nach außen.

Die Unterschiede zwischen Masquerading und SNAT sind:

- Bei Masquerading geben Sie nur ein Quellnetzwerk an. Es werden automatisch alle Dienste (Ports) in die Übersetzung mit einbezogen.
- Die Übersetzung findet nur dann statt, wenn das Paket über die angegebene Netzwerkkarte versendet wird. Als neue Quelladresse wird stets die Adresse dieser Netzwerkkarte in die Datenpakete eingefügt.

Damit eignet sich **Masquerading** besonders, um private Netzwerke in einem LAN hinter einer offiziellen IP-Adresse an das Internet anzubinden.

Masquerading definieren:

Legen Sie über die Drop-down-Menüs fest, welches Netzwerk auf welcher Netzwerkkarte maskiert werden soll. Im Normalfall wählt man die externe Netzwerkkarte.

Hinweis:

Damit von den Clients aus dem hier definierten Netzwerk eine Verbindung zum Internet aufgebaut werden kann, müssen im Menü **Packet Filter/Rules** die entsprechenden Regeln gesetzt werden. Das Setzen der Paketfilterregeln wird ausführlich in Kapitel 5.5 ab Seite 243 beschrieben.

---

1. Öffnen Sie im Verzeichnis **Network** das Menü **NAT/Masquerading**.

2. Vergeben Sie im Eingabefeld **Name** einen eindeutigen Namen für die **Masquerading-Regel**.

3. Wählen Sie im Drop-down-Menü **Rule Type** die Funktion **Masquerading** aus.

   Anschließend öffnet sich ein erweitertes Eingabefenster.

4. Wählen Sie im Drop-down-Menü **Network** ein Netzwerk aus.

5. Wählen Sie im Drop-down-Menü **Interface** eine Netzwerkkarte aus.

6. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

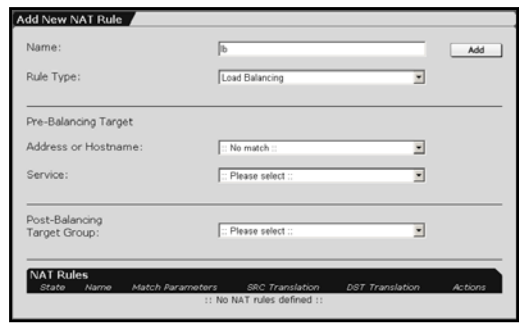
Nach erfolgreicher Definition wird die *Masquerading-Regel* in die Tabelle **NAT Rules** übernommen. Anschließend stehen Ihnen weitere Funktionen zur Verfügung.

Weitere Funktionen

Masquerading editieren: Durch einen Klick auf die Schaltfläche **edit** wird die Regel in das Fenster **Edit NAT Rule** geladen. Anschließend können Sie die Eingaben bearbeiten.

Masquerading löschen: Durch einen Klick auf die Schaltfläche **delete** wird der Eintrag aus der Tabelle gelöscht.

5.3.5.3. Load Balancing



Mit **Load Balancing** können Sie auf den Ports ankommende Datenpakete, z. B. SMTP oder HTTP auf verschiedene Server hinter dem Internet-Sicherheitssystem verteilen.

Beispiel: Sie haben in Ihrer DMZ zwei HTTP-Server mit den IP-Adressen 192.168.66.10 und 192.168.66.20. Mit *Load Balancing* können Sie nun die auf der externen Netzwerkkarte für den Dienst HTTP ankommenden Datenpakete auf die zwei HTTP-Server verteilen.

Bevor Sie die Load Balancing-Regel definieren können, müssen Sie im Menü **Definitions/Networks** die zwei HTTP-Server als Netzwerke, bestehend aus je einem Host, definieren und anschließend zu einer Netzwerkgruppe zusammenfassen.
Das Hinzufügen von Netzwerken (**Networks**) und die Erstellung von Netzwerkgruppen (**Network Groups**) wird in Kapiteln 5.2.1 ab Seite 134 schrieben.

Danach können Sie, wie nachfolgend beschrieben, die *Load Balancing*-Regel definieren.

Load Balancing definieren:

1. Öffnen Sie im Verzeichnis **Network** das Menü **NAT/Masquerading**.

2. Vergeben Sie im Eingabefeld **Name** einen eindeutigen Namen für die **Load-Balancing-Regel**.

   Anschließend öffnet sich ein erweitertes Eingabefenster.

3. Vergeben Sie im Eingabefeld **Name** einen eindeutigen Namen für die **Load-Balancing-Regel**.

4. Wählen Sie im Drop-down-Menü **Rule Type** die Funktion **Load Balancing** aus.

5. Wählen Sie im Fenster **Pre-Balancing Target** die original Zieladresse und den entsprechenden Dienst (**Service**) aus.

   Address or Hostname: Stellen Sie hier die original Ziel-Adresse ein. In der Regel ist dies die externe Adresse des Internet-Sicherheitssystems.

   Service: Wählen Sie hier den original Zielport (Dienst) aus.

6. Wählen Sie im Drop-down-Menü **Post-Balancing Target Group** die neue Adresse aus. In der Regel ist dies eine Netzwerkgruppe aus einzelnen Hosts.

Nach erfolgreicher Definition wird die Load-Balancing-Regel in die Tabelle **NAT Rules** übernommen. Anschließend stehen Ihnen weitere Funktionen zur Verfügung.

Weitere Funktionen

Load Balancing editieren: Durch einen Klick auf die Schaltfläche **edit** wird die Regel in das Fenster **Edit NAT Rule** geladen. Anschließend können Sie die Eingaben bearbeiten.

Load Balancing löschen: Durch einen Klick auf die Schaltfläche **delete** wird der Eintrag aus der Tabelle gelöscht.

5.3.6. DHCP Service



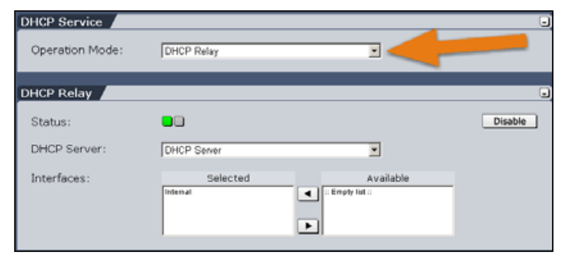
Das **Dynamic Host Configuration Protocol (DHCP)** weist den angeschlossenen Rechnern (Clients) aus einem festgelegten Bereich von IP-Adressen automatisch Adressen zu und spart so bei größeren Netzwerken viel Konfigurationsarbeit. Des Weiteren kann den Clients die Adresse des Default Gateways (Routers) und der zuständigen Nameserver (DNS) zugewiesen werden.

Neben der einfacheren Konfiguration der Clients und der Möglichkeit, mobile Rechner problemlos in unterschiedlichen Netzwerken zu betreiben, lassen sich in einem DHCP-Netzwerk Fehler einfacher lokalisieren, da die Konfiguration des Netzwerks, geht es um die Adressen, primär von der Konfiguration des DHCP-Servers abhängt. Außerdem lassen sich Adressbereiche effektiver nutzen, da keineswegs alle Hosts gleichzeitig im Netzwerk aktiv sind. Die IP-Adressen können so je nach Bedarf nacheinander an verschiedene Hosts vergeben werden.

Das Menü **DHCP Service** stellt zwei Betriebsmodi bereit. Im Modus **DHCP Relay** wird der Service von einem separaten DHCP-Server angeboten und das Sicherheitssystem fungiert als Relais. Im Modus **DHCP Server** wird der Adressbereich für das angeschlossene Netzwerk vom Sicherheitssystem bereitgestellt.

Die Konfiguration des Modus *DHCP Relay* wird im Anschluss beschrieben. Für den Betrieb im Modus *DHCP Server* werden die Grundeinstellungen und erweiterten Funktionen ab Seite 208 erklärt.

DHCP-Relay konfigurieren:



Bevor die Einstellungen für den Modus **DHCP Relay** durchgeführt werden können, muss der separate DHCP-Server im Menü **Definitions/ Networks** definiert werden.

1. Öffnen Sie im Verzeichnis **Network** das Menü **DHCP Service**.

2. Wählen Sie im Drop-down-Menü **Operation Mode** den Modus **DHCP Relay** aus.

   Das Fenster **DHCP Relay** wird geöffnet.

3. Schalten Sie die Funktion in der Zeile **Status** durch einem Klick auf die Schaltfläche **Enable** ein.

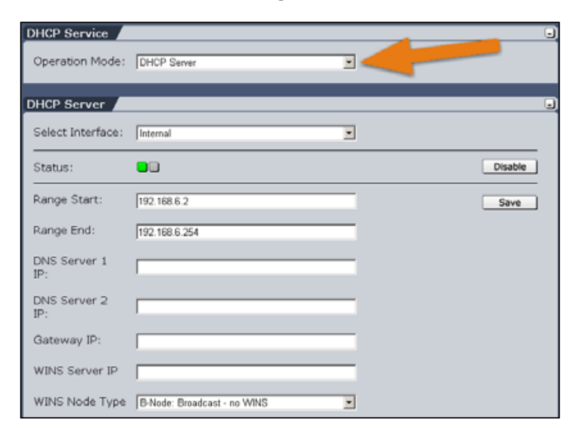
   Anschließend öffnet sich ein erweitertes Eingabefenster.

4. Wählen Sie im Drop-down-Menü **DHCP Server** den Server aus.

5. Wählen Sie im Auswahlfeld **Interfaces** die Schnittstellen aus, über die den Clients die IP-Adressen zugewiesen werden sollen.

Die Einstellungen werden anschließend ohne weitere Bestätigung übernommen.

DHCP-Server konfigurieren:



1. Öffnen Sie im Verzeichnis **Network** das Menü **DHCP Service**.
2. Wählen Sie im Drop-down-Menü **Operation Mode** den Modus **DHCP Server** aus.

   Das Fenster **DHCP Server** wird geöffnet.
3. Wählen Sie im Drop-down-Menü **Select Interface** die Schnittstelle aus, von der aus den Clients die IP-Adressen zugewiesen werden sollen.
4. Schalten Sie die Funktion in der Zeile **Status** durch einem Klick auf die Schaltfläche **Enable** ein.

   Anschließend öffnet sich ein erweitertes Eingabefenster.
5. Bestimmen Sie mit den Drop-down-Menüs **Range Start** und **Range End** den IP-Adressenbereich.

   Per Default wird im Eingabefeld der konfigurierte Adressbereich der Netzwerkkarte angezeigt.

Die Einstellungen werden anschließend ohne weitere Bestätigung übernommen.

DNS-Server, Gateway-IP und WINS-Server zuweisen:

Im Betriebsmodus **DHCP Server** können Sie den Clients weitere Parameter zur Netzwerkkonfiguration übergeben. Dazu gehören die DNS-Server-Adressen und das Default Gateway, welches die Clients verwenden sollen. In der Regel wird das Internet-Sicherheitssystem selbst diese Aufgaben übernehmen. In diesem Fall sollten Sie hier die interne Adresse Ihres Internet-Sicherheitssystems einstellen.

Die Konfiguration des DNS-Proxy erfolgt im Menü **Proxies/DNS**. Die Funktionalität des DNS-Proxy wird in Kapitel 5.6.4 ab Seite 336 beschrieben.

Für NetBIOS-Netzwerke kann zur Namensauflösung ein **WINS**-Server eingetragen werden. WINS ist die Abkürzung für Windows Internet Name Service. Ein WINS-Server ist ein MS Windows NT-Server, auf dem Microsoft TCP/IP und die WINS-Serversoftware ausgeführt werden. Auf WINS-Servern wird eine Datenbank verwaltet, in der Computernamen den IP-Adressen so zugeordnet werden, dass die Benutzer problemlos mit anderen Computern unter Benutzung der Windows-Techniken kommunizieren können und dabei alle Vorteile von TCP/IP nutzen können.

1. Öffnen Sie im Verzeichnis **Network** das Menü **DHCP Service**.

2. Tragen Sie in die Eingabefelder **DNS Server 1 IP** und **DNS Server 2 IP** die IP-Adressen der Nameserver ein.

3. Tragen Sie in das Eingabefeld **Gateway IP** die IP-Adresse des Default Gateways ein.

4. Falls Sie einen **WINS**-Server zuweisen möchten, führen Sie die folgenden zwei Einstellungen durch:

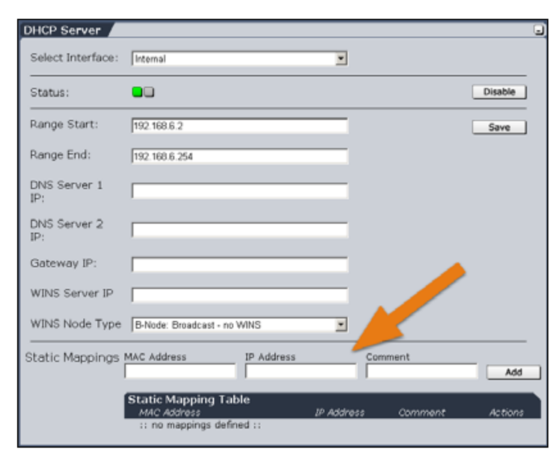
   WINS Server IP: Tragen Sie hier die IP-Adresse des WINS-Servers ein.

   WINS Node Type: Wählen Sie im Drop-down-Menü die Methode aus, die der Client zur Namensauflösung anwenden soll. Falls

die Einstellung **Do not set note type** ausgewählt ist, wird das Vorgehen vom Client selbst bestimmt.

5. Speichern Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

Statische Adresszuweisung konfigurieren:



Im Betriebsmodus **DHCP Server** können Sie einigen oder sogar allen Clients in diesem Netzwerk eine bestimmte IP-Adresse statisch zuweisen. Dafür benötigen Sie die MAC-Adresse der Netzwerkkarte dieses Clients.

1. Öffnen Sie im Verzeichnis **Network** das Menü **DHCP Service**.

2. Führen Sie im Fenster **Static Mappings** die folgenden Einstellungen durch:

   MAC Address: Tragen Sie in das Eingabefeld die MAC-Adresse der Netzwerkkarte ein. Die MAC-Adresse muss wie im Beispiel dargestellt eingegeben werden.
   Beispiel: 00:04:76:16:EA:62

   IP Address: Tragen Sie in das Eingabefeld die IP-Adresse ein. Diese IP-Adresse muss im Netzwerkbereich der internen Netzwerkkarte liegen.

   Comment: Über das Eingabefeld können Sie optional einen Kommentar für die statische Adresse hinzufügen.

3. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add**.

Anschließend wird die statische IP-Adresszuweisung in die Tabelle **Static Mapping Table** importiert. Durch einen Klick auf die Schaltfläche **delete** kann der Eintrag wieder gelöscht werden.

Current IP Leasing Table

Im Betriebsmodus **DHCP Server** werden in der Tabelle **Current IP Leasing** werden die aktuellen IP-Adresszuweisungen dargestellt. Für ein und dieselbe IP-Adresse können mehrere Zuweisungen enthalten sein, allerdings ist immer nur der letzte Eintrag gültig. Diese Tabelle wird nur angezeigt, wenn Einträge vorhanden sind.

5.3.7. PPTP VPN Access

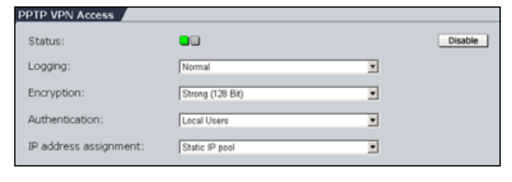
Mit **Point-to-Point Tunneling Protocol (PPTP)** können Sie einzelnen Hosts den Zugang zu Ihrem Netzwerk über einen verschlüsselten Tunnel ermöglichen. **PPTP** ist einfach einzurichten und benötigt auf Microsoft Windows Clients keine zusätzliche Software.

PPTP ist in Microsoft Windows ab Version 95 enthalten. Um **PPTP** mit dem Internet-Sicherheitssystem verwenden zu können, muss der Client die MSCHAPv2-Authentifizierung unterstützen. Zu diesem Zweck muss auf MS Windows 95 und 98 Clients ein Update aufgespielt werden. Dieses Update finden Sie bei Microsoft unter:

http://support.microsoft.com/support/kb/articles/Q191/5/40.ASP

Sie benötigen dort das VPN-Update und eventuell das RAS-Update, wenn Sie Microsoft Windows 95 verwenden.

PPTP VPN Access



In diesem Fenster schalten Sie den **PPTP-VPN**-Zugang durch einen Klick auf die jeweilige Schaltfläche **Enable**/ **Disable** ein- und aus.

Logging: Hier stellen Sie ein, wie ausführlich die Informationen in den **PPTP Logs** protokolliert werden. Stellen Sie den Protokollumfang auf **Ausführlich** (**Extensive**), wenn Verbindungsprobleme zum Host auftreten und öffnen anschließend das **Live Log**-Fenster. Sobald Sie nun die Verbindung starten, können Sie den Vorgang in Echtzeit verfolgen.

Das **PPTP Live Log** befindet sicht im Menü **Local Logs/Browse**.

Encryption: Hier stellen Sie die Verschlüsselungsstärke (40 Bit oder 128 Bit) dieser VPN-Verbindungsart ein. Beachten Sie, dass bei Microsoft Windows 2000 im Gegensatz zu Windows 98 und Windows

ME nur die Verschlüsselungsstärke 40 Bit installiert ist. Sie benötigen zusätzlich das **High Encryption Pack** oder **Service Pack 2**. **SP2** kann allerdings später nicht mehr deinstalliert werden.



Sicherheitshinweis:

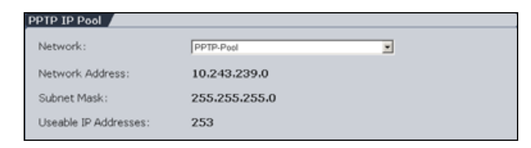
Stellen Sie im Drop-down-Menü **Encryption** die Verschlüsselungsstärke immer auf **Strong** (128 Bit) ein, es sei denn der Endpunkt (Host) unterstützt diese Verschlüsselungsstärke nicht.

Authentication: In diesem Drop-down-Menü stellen Sie die Authentifizierungsmethode ein. Wenn Sie im Menü **System/User Authentication** einen RADIUS-Server konfiguriert haben, können Sie hier auch RADIUS-Authentifizierung einsetzen.
Die Konfiguration des Microsoft IAS RADIUS-Servers und die Einstellungen im **WebAdmin** werden in Kapitel 5.1.8 ab Seite 83 erklärt.

IP Address Assignment: Mit dieser Funktion können Sie festlegen, ob den Hosts bei der Einwahl eine Adresse aus einem definierten **PPTP IP Pool** zugewiesen werden soll, oder ob die Adresse automatisch von einem **DHCP**-Server angefordert wird.
Bitte beachten Sie, dass der lokale DHCP-Server für diese Funktion nicht unterstützt wird. Der DHCP-Server muss physikalisch auf einem anderen System laufen.

Alternativ zu den beiden Optionen kann jedem Benutzer eine bestimmte IP-Adresse zugeteilt werden. Dafür muss für jeden dieser Benutzer im Menü **Definitions/Users** ein Account angelegt werden. Die zugeteilte IP-Adresse muss nicht aus dem *IP Pool* stammen. Bei der Einwahl wird dem Host diese Adresse dann automatisch zugewiesen.

PPTP IP Pool



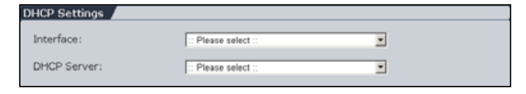
Hier legen Sie fest, welche IP-Adressen den Hosts vom **Static PPTP IP Pool** bei der Einwahl zugewiesen werden. Per Default-Einstellung wird beim ersten Aktivieren der PPTP-Funktion ein Netzwerk aus dem privaten IP-Bereich 10.x.x.x ausgewählt. Dieses Netzwerk wird **PPTP Pool** genannt und kann für alle anderen Funktionen des Internet-Sicherheitssystems genutzt werden, in denen Netzwerkdefinitionen verwendet werden. Falls Sie ein anderes Netzwerk verwenden wollen, können Sie entweder die bestehende *PPTP Pool*-Definition verändern, oder ein anderes definiertes Netzwerk als *PPTP Pool* festlegen.

Die PPTP-Benutzer legen Sie im Menü **Definitions/Users** an. Dort ist es möglich, bestimmten Benutzern eigene IP-Adressen zuzuweisen. Diese IP-Adressen müssen nicht Bestandteil des verwendeten Pools sein. Sollen diese Adressen im Paketfilter oder an anderer Stelle der Konfiguration verwendet werden, müssen sie entweder als einzelne Hosts (Netzmaske 255.255.255.255) oder als Teil eines übergeordneten Netzwerkes definiert werden.

Hinweis:

Falls Sie für Ihren **PPTP Pool** private IP-Adressen, wie z. .B. das vordefinierte Netzwerk verwenden, müssen Sie **Masquerading** oder **NAT**-Regeln für den *PPTP Pool* erstellen, wenn ein Zugriff auf das Internet von den PPTP-Hosts aus erwünscht ist.

DHCP Settings

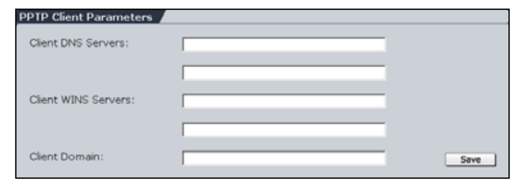


Dieses Fenster wird angezeigt, wenn Sie im Fenster **PPTP VPN Access** bei der Funktion **IP Address Assignment** die Einstellung **DHCP** ausgewählt haben.

Interface: Stellen Sie hier die Netzwerkkarte ein, über die der DHCP-Server angeschlossen ist. Beachten Sie dabei, dass der DHCP-Server nicht direkt angeschlossen sein muss – der Zugang ist ebenso über einen Router möglich.

DHCP Server: Wählen Sie hier den DHCP-Server aus. In diesem Drop-down-Menü werden alle Hosts angezeigt, die im Menü **Definitions/Networks** definiert wurden.

PPTP Client Parameters



In diesem Fenster können Sie den Hosts während des PPTP-Verbindungsaufbaus zusätzlich bestimmte Nameserver (DNS und WINS) und eine Name-Service-Domäne zuweisen.

Verbindung mit MS Windows 2000:

Hier wird in einem Beispiel-Szenario beschrieben, wie eine Verbindung mit PPTP VPN Access konfiguriert wird, wenn auf dem Host Microsoft Windows 2000 installiert ist.

1. Öffnen Sie im Verzeichnis **Network** das Menü **PPTP VPN**.

2. Schalten Sie im Fenster **PPTP VPN Access** die Funktion durch einen Klick auf die Schaltfläche **Enable** ein.

Die Statusampel zeigt Grün und ein erweitertes Eingabefenster wird geöffnet.

3. Führen Sie im Fenster **PPTP VPN Access** die Einstellungen für den Netzwerkzugang durch:

Logging: Behalten Sie die Einstellung **Normal** bei.

Encryption: Bestimmen Sie im Drop-down-Menü die Verschlüsselungsstärke. Sie können zwischen **weak (40 Bit)** und **strong (128 Bit)** wählen.

Beachten Sie, dass bei Microsoft Windows 2000 im Gegensatz zu MS Windows 98 und Windows ME nur die Verschlüsselungsstärke 40 Bit standardmäßig installiert ist.
Für eine 128 Bit-Verschlüsselungsstärke benötigen Sie zusätzlich das **High Encryption Pack** oder **Service Pack 2**. **SP2** kann aber später nicht mehr deinstalliert werden. Die ausgewählte Verschlüsselungsstärke wird sofort übernommen.

Wichtiger Hinweis:

Damit die Verbindung zustande kommt, muss auf beiden Seiten die gleiche Verschlüsselungsstärke eingestellt sein. Wenn im **WebAdmin** die Verschlüsselungsstärke 40 Bit eingestellt ist und Sie auf der Gegenstelle in MS Windows 2000 die Verschlüsselungsstärke 128 Bit auswählen, kommt fälschlicherweise die Meldung unter Windows, dass die Verbindung besteht.

Authentication: Stellen Sie im Drop-down-Menü die Authentifizierungsmethode ein.

4. Legen Sie fest, welche IP-Adressen den Hosts bei der Einwahl zugewiesen werden sollen. Wählen Sie im Fenster **PPTP IP Pool** mit dem Drop-down-Menü **Network** ein Netzwerk aus. Das ausgewählte Netzwerk wird sofort übernommen.
   Per Default-Einstellung ist hier bereits **PPTP Pool** ausgewählt.

   Anschließend wird unter dem Drop-down-Menü die IP-Adresse des Netzwerks, die Netzwerkmaske und die Anzahl der verfügbaren IP-Adressen angezeigt.
   Dem Benutzer wird bei der Einwahl aus diesem Adressbereich automatisch eine IP-Adresse zugeordnet.

5. Im Fenster **PPTP Client Parameters** können Sie den Hosts während des PPTP-Verbindungsaufbaus zusätzlich bestimmte Nameserver (DNS und WINS) und eine Name-Service-Domäne zuweisen. Es können jeweils zwei Server eingetragen werden.

   Client DNS Servers: Tragen Sie hier die IP-Adressen der DNS-Server ein.

   Client WINS Servers: Tragen Sie hier die IP-Adressen der Windows-Nameserver ein.

   Client Domain: Tragen Sie hier die Domain ein, die der Client bei DNS-Anfragen an Hostnamen anhängen soll.

6. Speichern Sie die Eingaben durch einen Klick auf die Schaltfläche **Save**.

Die weitere Konfiguration erfolgt am Host des Benutzers. Der Benutzer benötigt zur weiteren Konfiguration die IP-Adresse des Servers sowie einen Benutzernamen und Passwort. Diese Angaben werden vom Administrator des Internet-Sicherheitssystems vergeben.

1. Klicken Sie in Microsoft Windows 2000 auf **Start/Einstellungen/Netzwerk und DFÜ-Verbindungen**.

2. Klicken Sie auf das Icon **Neue Verbindung erstellen**.

   Der **Netzwerksverbindungs-Assistent** öffnen sich.

   Klicken Sie anschließend auf die Schaltfläche **Weiter**.

3. Wählen Sie die folgende Option aus: **Verbindung mit einem privaten Netzwerk über das Internet herstellen.**

   Klicken Sie anschließend auf die Schaltfläche **Weiter**.

4. Falls Sie eine permanente Verbindung ins Internet haben, wählen Sie die folgende Option aus: **Keine Anfangsverbindung automatisch wählen**.

   Klicken Sie anschließend auf die Schaltfläche **Weiter**.

   Falls Sie sich zuerst über einen Provider in das Internet einwählen, klicken Sie auf die Option **Andere Verbindung zuerst wählen** und wählen im Auswahlmenü Ihren Provider aus. Diese Einstellungen können Sie auch später im Dialog **Eigenschaften** vornehmen bzw. ändern.

5. Tragen Sie in das Eingabefeld **Zieladresse** die IP-Adresse des Servers ein.

   Klicken Sie anschließend auf die Schaltfläche **Weiter**.

6. Bestimmen Sie im Fenster **Verfügbarkeit der Verbindung** ob der PPTP-Zugang für alle Benutzer oder nur für Sie selbst zu Verfügung stehen soll.

   Klicken Sie anschließend auf die Schaltfläche **Weiter**.

7. Geben Sie im Fenster **Fertigstellen des Assistenten** in das Eingabefeld einen beliebigen Namen für die PPTP-Verbindung ein.

   Klicken Sie anschließend auf die Schaltfläche **Weiter**.

8. Mit einem Klick mit der rechten Maustaste auf das neue Symbol im Menü **Start / Einstellungen / Netzwerk und DFÜ-Verbindungen** können Sie im Dialog **Eigenschaften** in verschiedenen Registerkarten weitere Einstellungen vornehmen oder ändern:

   Allgemein: Hier können Sie den Hostnamen oder die Ziel-IP-Adresse ändern. Falls vor der PPTP-Verbindung eine Verbindung zum Internet Service Provider (ISP) aufgebaut werden muss, stellen Sie diese im Fenster **Erste Verbindung** ein.

   Optionen: Hier können Sie die Wähl- und Wahlwiederholungsoptionen definieren.

   Sicherheit: Wählen Sie die Option **Erweitert (Benutzerdefinierte Einstellungen)**. Klicken Sie anschließend auf die Schaltfläche **Einstellungen**. Belassen Sie die Standardeinstellungen in diesem Menü.

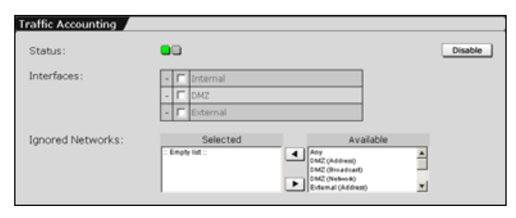
   Netzwerk: Wählen Sie im Auswahlmenü **Typ des anzurufenden VPN-Servers** die Option **Point-to-Point-Tunneling-Protokoll (PPTP)** aus.

   Gemeinsame Nutzung: Hier können Sie die Nutzungsbedingungen für die PPTP-Verbindung definieren.

Anschließend wird die PPTP-Verbindung mit einem Klick auf das neue Icon im Menü **Start / Einstellungen / Netzwerk und DFÜ-Verbindungen** gestartet.

Weitere Informationen erhalten Sie in der Regel vom Administrator des Netzwerks.

5.3.8. Accounting



Mit dem **Accounting** werden auf den Netzwerkkarten alle transportierten IP-Pakete erfasst und die Datenmenge aufsummiert. In diesem Menü können Sie spezifizieren, auf welchen Netzwerkkarten der anfallende Datenverkehr gezählt werden soll. Sie haben die Möglichkeit, die gesammelten Daten im Menü **Log Files / Accounting** herunterzuladen, oder eine tägliche Auswertung der Daten im Menü **Reporting / Accounting** zu konfigurieren.

Wichtiger Hinweis:

Im Normalfall sollte das **Accounting** nur auf einer Netzwerkkarte durchgeführt werden, da sonst weitergeleitete Datenpakete mehrmals gezählt werden.

Wenn Sie **Masquerading** verwenden, sollten Sie das **Accounting** auf der internen Netzwerkkarte durchführen. Datenpakete, die auf der externen Netzwerkkarte das Internet-Sicherheitssystem verlassen, wurden bereits auf die neue Quelladresse umgeschrieben.

Sie haben auch die Möglichkeit, **Hosts** oder **Netzwerke** vom **Accounting** auszuschließen. Nach Installation des Internet-Sicherheitssystems sind alle Netzwerke in die Accounting-Funktion einbezogen.

Netzwerk vom **Accounting** auszuschließen könnte von Interesse sein, wenn z. B. die Netzwerkkarte zur **DMZ** im **Accounting** eingetragen ist, aber ein einzelner Rechner im **DMZ** nicht mitgezählt werden soll. Da er eventuell nur für interne Zwecke genutzt wird, macht es keinen Sinn, seine Traffic-Daten in die Abrechnung einzubeziehen.

Im Menü **Reporting / Accounting** können Sie nach entsprechender Definition das **Accounting** beobachten.

Wichtiger Hinweis:

Führen Sie das **Accounting** nicht auf **Gigabit**-Netzwerkkarten aus. Durch die hohen Datenmengen kann diese Funktion sonst zu einer Auslastung des Prozessors (CPU) führen.

Traffic Accounting einstellen:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Accounting**.

2. Schalten Sie die Funktion durch einen Klick auf die Schaltfläche **Enable** ein.

   Die Statusampel zeigt Grün und ein erweitertes Eingabefenster wird geöffnet.

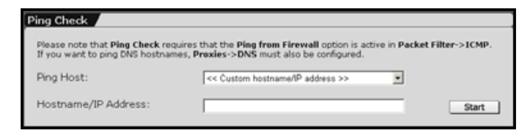
3. Wählen Sie in der Auswahltabelle **Interfaces** die Netzwerkkarten aus.

   Die Funktionsweise der **Auswahltabelle** wird in Kapitel 4.3.3 ab Seite 42 beschrieben.

4. Wählen Sie im Auswahlfeld **Ignored Networks** die Netzwerke aus, die vom Traffic Accounting nicht berücksichtigt werden sollen.

Die Einstellungen im Menü **Traffic Accounting** werden sofort übernommen.

5.3.9. Ping Check



Mit der Aktion **Ping** können Sie die Verbindung zu einem entfernten Host auf IP-Ebene testen. Für die Aktion muss im Menü **Packet Filter/ICMP** die Funktion **ICMP on Firewall** aktiviert sein. Das Programm **Ping** verschickt an einen anderen Rechner ein **ICMP-Echo-Paket**. Wenn der Rechner das ICMP-Echo-

Paket erhält, muss sein TCP-IP-Stack ein **ICMP-Echo-Reply-Paket** an den Absender zurückschicken. So können Sie feststellen, ob eine Verbindung zu einem anderen Netzwerk-Rechner möglich ist.

Mit **Ping Check** können Sie die Verbindung zu einem Host auch durch Eingabe des DNS-Hostnamens testen. Dafür muss im Menü **Proxies/DNS** der **DNS-Proxy** eingeschaltet sein.

Hinweis:

- Für das Tool **Ping** muss im Menü **Packet Filter/ICMP** die Funktion **ICMP on Firewall** eingeschaltet sein.
- Für die **Namensauflösung** (**Name Resolution**) muss im Menü **Proxies/DNS** der **DNS-Proxy** eingeschaltet und konfiguriert sein.

Ping starten:

1. Öffnen Sie im Verzeichnis **Network** das Menü **Ping Check**.
2. Wählen Sie im Drop-down-Menü **Ping Host** die Netzwerkarte aus.

   Falls es sich bei der Schnittstelle um eine in den Menüs **Interfaces** oder **Networks** konfigurierten Host handelt, können Sie diese im Drop-down-Menü direkt auswählen.
   (Beispiel: **Internal (Address)** für die interne Netzwerkkarte auf dem Internet-Sicherheitssystem)

   Für einen anderen Host im Netzwerk wählen Sie im Drop-down-Menü die Einstellung **Custom Hostname/IP Address** aus.
3. Tragen Sie in das Eingabefeld **Hostname/IP Address** die IP-Adresse oder den Hostnamen ein.
4. Starten Sie die Testverbindung durch einen Klick auf die Schaltfläche **Start**.

5.4. Intrusion Protection

Das Modul **Intrusion Protection System (IPS)** erkennt Angriffsversuche anhand eines signaturbasierten Intrusion-Detection-Regelwerks. Das System analysiert den gesamten Datenverkehr und blockiert u. a. Attacken automatisch, bevor diese das lokale Netzwerk erreichen.

Die bereits vorhandene Basis an Regeln, bzw IPS-Angriffssignaturen wird durch die Funktion **Pattern Up2Date** aktualisiert. Neue IPS-Angriffssignaturen werden automatisch als IPS-Regel in das IPS-Regelwerk importiert.

5.4.1. Settings

Global Settings



In diesem Fenster führen Sie die Grundeinstellungen für das Modul **Intrusion Protection System** (**IPS**) durch.

Status: Durch einen Klick auf die Schaltfläche **Enable** schalten Sie das Modul ein.

Local Networks: Wählen Sie im Auswahlfeld die Netzwerke aus, die vom *Intrusion Protection System (IPS)* überwacht werden sollen. Falls kein Netzwerk ausgewählt ist, wird der gesamte Datenverkehr überwacht.

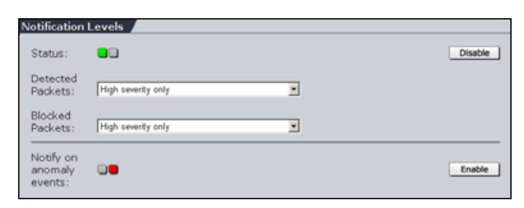
Anomaly Detection



Die Funktion **Anomaly Detection** analysiert den Datenverkehr statistisch und heuristisch. Sie überwacht den gesamten Datenverkehr Im Netzwerk und speichert dabei die gebräuchlichsten

Dienste sowie die verfügbaren Hosts. Wenn ein ungewöhnlicher Datenverkehr, Dienst oder Host entdeckt wird, schickt das Modul eine entsprechende Warnung ab. Es wird ebenfalls eine Warnung verschickt, wenn Datenpakete auftauchen, die auf einen Angriff hinweisen. Alle Vorfälle werden im Intrusion Protection log protokolliert.
Die Funktionen Schalten Sie durch einen Klick auf die Schaltfläche **Enable** ein.

Notification Levels



Falls das **Intrusion Protection System (IPS)** eine IPS-Angriffssignatur erkennt oder einen Intrusion-Vorfall verhindert, wird vom System per E-Mail eine entsprechende Warnung an den Administrator abgeschickt. Die E-Mail-Adresse des Administrators wird im Menü **System / Settings** eingestellt.

Detected Packets: Stellen Sie in diesem Drop-down-Menü ein, ab welcher Gefahrenstufe der Alarmierungsregel eine Warnung abgeschickt wird (Intrusion Detection).

- **All levels**: Bei jeder Gefahrenstufe.
- **High and medium severity**: Bei hoher und mittlerer Gefahrenstufe.
- **High serverity only**: Nur bei hoher Gefahrenstufe.
- **None**: Es wird keine Warnung versendet.

Blocked Packets: Stellen Sie in diesem Drop-down-Menü ein, ab welcher Gefahrenstufe der Blockierungsregel eine Warnung abgeschickt wird (Intrusion Prevention).

- **All levels**: Bei jeder Gefahrenstufe.
- **High and medium severity**: Bei hoher und mittlerer Gefahrenstufe.
- **High serverity only**: Nur bei hoher Gefahrenstufe.
- **None**: Es wird keine Warnung versendet.

Notify on anomaly events: Wenn die Funktion **Anomaly Detection** eingeschaltet ist, werden bei außergewöhnlichen Ereignissen Notification E-Mails erstellt und abgeschickt.
Die Funktion wird durch einen Klick auf die Schaltfläche Enable eingeschaltet (Statusampel zeigt grün).

5.4.2. Rules

Das Menü **Rules** enthält das **Intrusion-Protection-System**-Regelwerk (**IPS**). Das bereits vorhandene Basisregelwerk mit den IPS-Angriffssignaturen wird auf Wunsch durch die Funktion **Pattern Up2-Date** aktualisiert. Neue IPS-Angriffssignaturen werden automatisch als IPS-Regel in die IPS-Regeltabelle importiert.

Die Funktion **Pattern Up2Date** wird in Kapitel 5.1.3 ab Seite 60 beschrieben.

Die IPS-Regel-Übersicht

In der Übersicht sind alle IPS-Regelgruppen enthalten.

Intrusion Protection Rules — Total 2012 entries, 1968 filtered — ▽ New Rule ... ▽ — ▽ Filters ▽

			▽ Group	Hits	Info
			attack-responses	0	Recognition of successful attacks
			backdoor	0	Rules for backdoor software
			bad-traffic	0	Recognizes traffic that should never occur
			chat	0	Recognition of messaging and chat traffic
			ddos	0	Rules for Distributed Denial of Service
			dns	0	Rules for DNS protocol
			dos	0	Denial of Service attacks
			exploit	0	Well-known exploits of specific software
			finger	0	Rules for finger protocol
			ftp	0	Rules for FTP protocol
			icmp	0	Rules for ICMP protocol
			icmp-info	0	Recognition of assumingly harmless ICMP traffic

Die Funktionen in der Übersicht von links nach rechts:

/ : Durch einen Klick auf die Statusampel wird die IPS-Regelgruppe ein- und ausgeschaltet.

/ : Die IPS-Regel kann als Alarmierungsregel (Intrusion Detection) oder als Blockierungsregel (Intrusion Prevention) eingestellt werden. Durch einen Klick auf das Symbol werden alle IPS-Regeln in dieser Gruppe umgeschaltet.

: Durch einen Klick auf das Ordner-Symbol wird das Unterverzeichnis mit allen Protokollen dieser Gruppe angezeigt.
Durch einen nochmaligen Klick auf das Symbol gelangen Sie wieder in die Übersicht. Die zusätzlichen Funktionen im Unterverzeichnis werden im Abschnitt „Das IPS-Regel-Unterverzeichnis“ beschrieben.

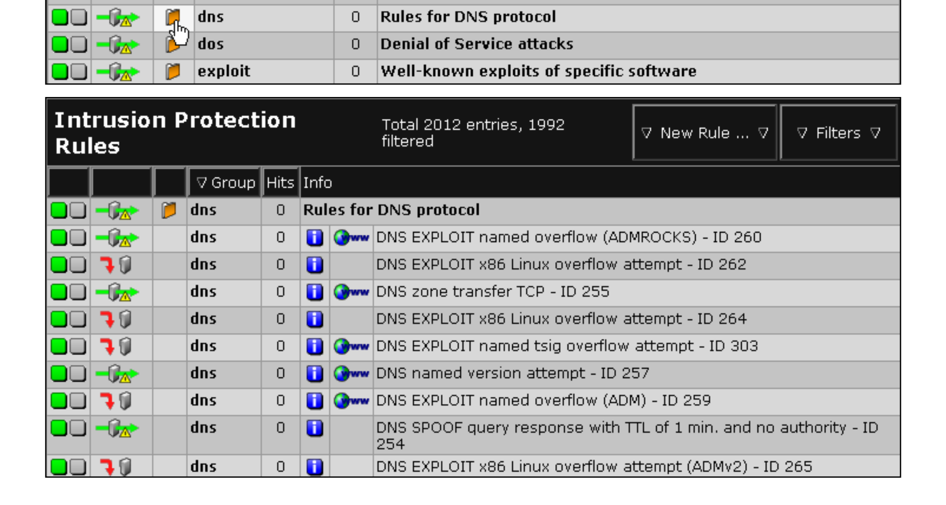
Group: In dieser Spalte wird der Name der IPS-Regelgruppe angezeigt. Die Gruppen sind anhand dieses Namens alphabetisch sortiert. Durch einen Klick in die Kopfzeile werden die Gruppen alphabetisch auf- oder absteigend dargestellt.

Hits: In dieser Spalte wird angezeigt, wie oft eine Regel aus dieser Gruppe aktiv wurde.

Info: In dieser Spalte erhalten Sie eine kurze Information zu dieser IPS-Regelgruppe.

Das IPS-Regel-Unterverzeichnis

Im Unterverzeichnis befinden sich alle IPS-Regeln einer Gruppe. Die Untergruppe wird in der Übersicht durch einen Klick auf das Ordner-Symbol () geöffnet.



Group	Hits	Info
ddos	0	Rules for Distributed Denial of Service
dns	0	Rules for DNS protocol
dos	0	Denial of Service attacks
exploit	0	Well-known exploits of specific software

Intrusion Protection Rules — Total 2012 entries, 1992 filtered — ▽ New Rule ... ▽ — ▽ Filters ▽

▽ Group	Hits	Info
dns	0	Rules for DNS protocol
dns	0	DNS EXPLOIT named overflow (ADMROCKS) - ID 260
dns	0	DNS EXPLOIT x86 Linux overflow attempt - ID 262
dns	0	DNS zone transfer TCP - ID 255
dns	0	DNS EXPLOIT x86 Linux overflow attempt - ID 264
dns	0	DNS EXPLOIT named tsig overflow attempt - ID 303
dns	0	DNS named version attempt - ID 257
dns	0	DNS EXPLOIT named overflow (ADM) - ID 259
dns	0	DNS SPOOF query response with TTL of 1 min. and no authority - ID 254
dns	0	DNS EXPLOIT x86 Linux overflow attempt (ADMv2) - ID 265

Die Funktionen im Unterverzeichnis von links nach rechts:

/ : Durch einen Klick auf die Statusampel wird die IPS-Regel ein- und ausgeschaltet.

/ : Die IPS-Regel kann als Alarmierungsregel (Intrusion Detection) oder als Blockierungsregel (Intrusion Prevention) eingstellt werden. Durch einen Klick auf das Symbol wird die IPS-Regel umgeschaltet.

: Durch einen Klick auf das Ordner-Symbol kehren Sie in die Übersicht zurück.

Group: In dieser Spalte wird der Name der IPS-Regelgruppe angezeigt.

Hits: In dieser Spalte wird angezeigt, wie oft eine Regel aus dieser Gruppe aktiv wurde.

Info: In der ersten Zeile erhalten Sie eine kurze Information zu dieser IPS-Regelgruppe. Zu den einzelnen IPS-Regeln erhalten Sie ausführliche Informationen, indem Sie mit der Maus das entsprechende Symbol berühren.

: In diesem Fenster werden die Parameter dieser Regel als Low Layer Information dargestellt.

www: Durch einen Klick auf das Symbol werden Sie mit dem entsprechenden Link im Internet verbunden. Auf der Internetseite erhalten Sie weitere Informationen zu der IPS-Regel. Die Informationen werden z. B. in Projekten wie Common Vulnerabilities and Exposures (CVE) erarbeitet und im Internet veröffentlicht.

IPS-Regel setzen:

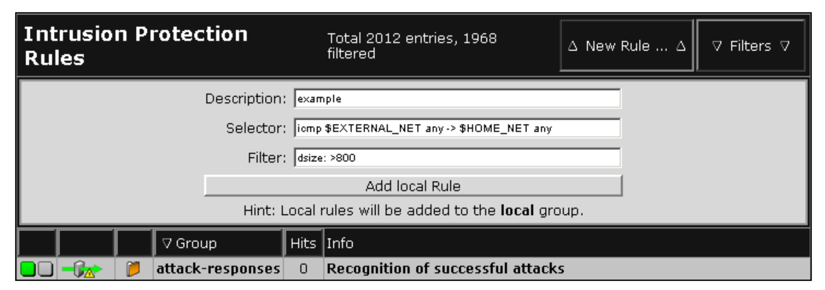
Das Regelwerk kann durch eigene IPS-Regeln ergänzt werden. Die Regeln basieren auf der Syntax des Open-Source-ID-Systems Snort. Manuell erstellte IPS-Regeln werden immer in IPS-Regelgruppe **local** importiert. Weitere informationen erhalten Sie unter der folgenden Internetadresse: http://www.snort.org.

1. Öffnen Sie im Verzeichnis **Intrusion Protection** das Menü **Rules**.

2. Klicken Sie auf die Schaltfläche **New Rule**.

   Anschließend wird das Eingabefenster geöffnet.

3. Führen Sie die folgenden Einstellungen durch:



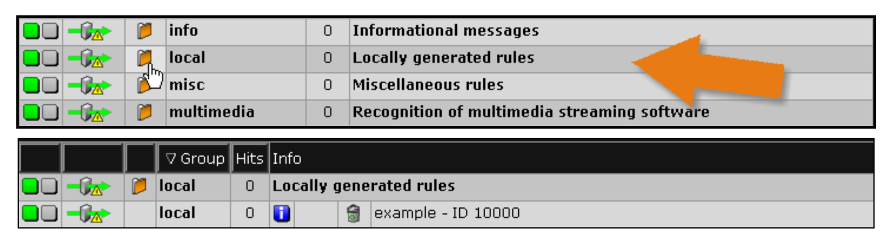
   Description: Tragen Sie in das Eingabefeld eine Beschreibung der Regel ein.
   Beispiel: `Large ICMP packet/großes ICMP-Datenpaket`

   Selector: Tragen Sie in das Eigabefeld die Auswahlparameter für die IPS-Regel in der Snort-Syntax ein.
   Beispiel: `icmp $EXTERNAL_NET any -> $HOME_NET any`

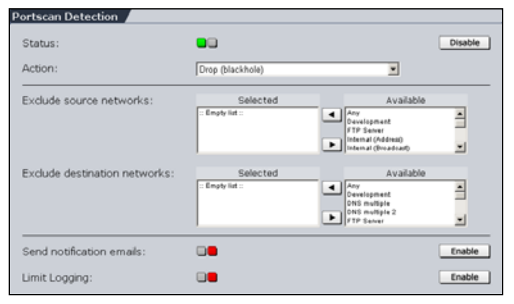
   Filter: Tragen Sie in das Eigabefeld die eigentliche Erkennung für die IPS-Regel in der Snort-Syntax ein. Achten Sie darauf, dass der Eintrag mit einem **;**-Zeichen beendet wird.
   Beispiel: `dsize: >800;`

4. Speichern Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add local Rule**.

Die neue **IPS-Regel** wird immer in die IPS-Regelgruppe **local** importiert. Die Regel ist sofort eingeschaltet (Statusampel zeigt Grün).



5.4.3. Portscan Detection



Mit **Portscan Detection** oder auch **PSD** sind Sie in der Lage, mögliche Angriffe durch Unbefugte zu erkennen. Sogenannte Portscans werden meist von Hackern durchgeführt, um ein abgesichertes Netzwerk nach erreichbaren *Diensten (Services)* zu durchsuchen. Um in ein System einzudringen bzw. eine **Denial-of-Service (DoS)**-Attacke zu starten, benötigt der Angreifer Informationen zu den Netzwerk-Diensten. Wenn solche Informationen vorliegen, ist der Angreifer möglicherweise in der Lage, gezielt die Sicherheitslücken dieser Dienste auszunutzen. Netzwerkdienste, die die Internet-Protokolle TCP und UDP verwenden, sind über bestimmte Ports erreichbar und diese Port-Zuordnung ist im Allgemeinen bekannt, z. B. ist der Dienst SMTP in der Regel dem TCP Port 25 zugeordnet. Die von Diensten verwendeten Ports werden als „offen“ (open) bezeichnet, da es möglich ist, eine Verbindung zu ihnen aufzubauen. Die unbenutzten Ports werden hingegen als „geschlossen“ (closed) bezeichnet – Versuche zu ihnen eine Verbindung aufzubauen scheitern. Damit nun der Angreifer herausfinden kann, welche Ports

„offen“ sind, verwendet er ein spezielles Software-Tool, den Port Scanner. Dieses Programm versucht mit mehreren Ports auf dem Zielrechner eine Verbindung aufzubauen. Falls dies gelingt, meldet es die entsprechenden Ports als „offen“ und der Angreifer hat die nötigen Informationen, welche Netzwerkdienste auf dem Zielrechner verfügbar sind.

Der Port Scanner kann z. B. folgende Informationen liefern:

```
Interesting ports on (10.250.0.114):
          (The 1538 ports scanned but not shown below are
          in state: closed)
          Port       State    Service
          25/tcp     open     smtp
          135/tcp    open     loc-srv
          139/tcp    filtered netbios-ssn
          445/tcp    open     Microsoft-ds
          1032/tcp   open     iad3
```

Da den Internetprotokollen TCP und UDP je 65535 Ports zur Verfügung stehen, werden die Ports in sehr kurzen Zeitabständen gescannt. Wenn nun von derselben IP-Adresse mehrere Versuche registriert werden, mit immer anderen Ports Ihres Systems Verbindung aufzunehmen bzw. Informationen an diese zu senden, dann handelt es sich mit ziemlicher Sicherheit um einen Portscan.

PSD entdeckt diese Portscans und informiert per E-Mail den Administrator sobald der Vorgang protokolliert wurde. Anschließend können Sie entscheiden, welche Maßnahme gegen weitere Verbindungen vom Port Scanner des Angreifers durchgeführt werden soll.

Die E-Mail-Adresse des Administrators wird im Menü **System / Settings** eingestellt.



Sicherheitshinweis:

Achten Sie als Administrator darauf, dass auf dem System immer die aktuellsten Sicherheits-Patches eingespielt sind.
Der Up2Date-Service wird ausführlich in Kapitel 5.1.3 ab Seite 60 beschrieben.

Portscan Detection einschalten / ausschalten:

1. Öffnen Sie im Verzeichnis **Intrusion Protection** das Menü **Portscan Detection**.

2. Schalten Sie die Funktion durch einem Klick auf die Schaltfläche **Enable** bei **Status** ein.

   Anschließend öffnet sich das Fenster **Portscan Detection**.

3. Wählen Sie im Drop-down-Menü **Action** die Maßnahme gegen den erkannten Portscanner aus.

   Accept: Es wird keine Maßnahme gegen den Portscanner ergriffen – es erfolgt nur eine Meldung.

   Obwohl diese Einstellung keine Maßnahmen gegen den Portscanner einleitet, ist dies die Standardeinstellung. Unter Umständen kann es vorkommen, dass auch normale Netzwerkaktivitäten als ein Portscan interpretiert werden. Die restriktiven Maßnahmen können in diesem Fall die Arbeit behindern.

   Drop (blackhole): Die nachfolgenden Pakete einer Portscansequenz werden verworfen und es kommt keine Verbindung zu Stande. Für den Portscanner ist dieser Port „gefiltert“ (filtered).

   Reject (reply with icmp unreachable): Die Verbindungsanfragen des Angreifers werden mit einem RST ACK „port unreachable“ zurückgewiesen. Dadurch wird der Port als „geschlossen“ (closed) ausgegeben und dem Angreifer bleiben die Dienste (Services) versperrt.

Falls Sie **Drop** oder **Reject** ausgewählt haben, bleibt die gewählte Aktion solange in Kraft, bis der portscan-typische Datenverkehr aufhört.

4. Mit den folgenden beiden Einstellungen können Sie Netzwerke von der Funktion *Portscan Detection* auschließen.

Exclude Source Networks: Hier können Sie zuverlässige Quellnetzwerke auswählen, die von der Funktion ausgeschlossen werden sollen.

Exclude Destination Networks: Hier können Sie zuverlässige Zielnetzwerke auswählen, die von der Funktion ausgeschlossen werden sollen.

5. Wenn der Administrator bei einem entdeckten Portscan per E-Mail informiert werden soll, schalten Sie die Funktion **Send Notification E-Mails** ein.

Die E-Mail-Adresse des Administrators wird im Menü **System/ Settings** eingestellt.

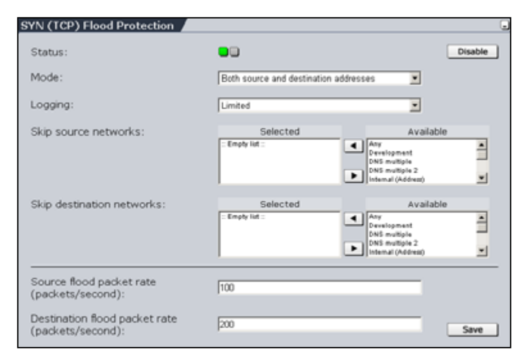
6. Wenn den Protokollumfang minimieren möchten, schalten Sie die Funktion **Limit Logging** ein.

Während eines Portscans können in der entsprechen Log-Datei viele unterschiedliche Einträge gemacht werden. Durch diese Funktion können Sie den Protokollumfang auf das Nötigste herabsetzen. Die Log-Dateien werden im Menü **Local Logs/ Browse** verwaltet.

5.4.4. DoS/Flood Protection

Mit den Funktionen in diesem Menü können **Denial-of-Service**-(**DoS**)- und **Distributed-Denial-of-Service**-(**DDoS**)-Angriffe abgewehrt werden, indem der Umfang der SYN-(TCP)-, UDP- und ICMP-Pakete, die in das Netzwerk geschickt werden, über eine bestimmte Zeit begrenzt werden.

SYN (TCP) Flood Protection



Die **Denial-of-Service**-Angriffe (**DoS**) auf Server zielen darauf ab, legitimen Nutzern den Zugriff auf einen Dienst zu verwehren. Im einfachsten Fall überflutet der Angreifer den Server mit sinnlosen Paketen, um Ihre Leitung zu überlasten. Da für diese Angriffe eine große Bandbreite erforderlich ist, verlegen sich immer mehr Angreifer auf sogenannte SYN-Flood-Attacken, die nicht darauf abzielen, die Bandbreite auszulasten, sondern die Systemressourcen des Servers selbst zu blockieren. Dazu verschicken sie sogenannte SYN-Pakete an den TCP-Port des Dienstes, bei einem Web-Server also auf Port 80.

Durch die Funktion **SYN (TCP) Flood Protection** wird die Anzahl der SYN-Pakete, die in das lokale Netzwerk gesendet werden, begrenzt. Per Default ist die Funktion ausgeschaltet (Statusampel zeigt Rot).

SYN (TCP) Flood Protection:

1. Öffnen Sie im Verzeichnis **Intrusion Protection** das Menü **DoS Flood Protection**.

2. Schalten Sie die Funktion durch einem Klick auf die Schaltfläche **Enable** bei **Status** ein.

   Anschließend öffnet sich ein erweitertes Eingabefenster.

3. Wählen Sie im Drop-down-Menü **Mode** den Modus aus.

   Both source and destination addresses: In diesem Modus werden SYN-(TCP)-Pakete zurückgewiesen, die sowohl die Quell-IP-adresse als auch die Ziel-IP-Adresse behandeln: zuerst werden die SYN-Pakete für die Quelladresse gefilter. Wenn dann noch zu viele Anfragen vorhanden sind, werden zusätzlich die SYN-Pakete für die Zieladresse gefiltert.

   Destination address only: In diesem Modus werden nur die SYN-(TCP)-Pakete zurückgewiesen, die speziell die Ziel-IP-Adresse behandeln.

   Source address only: In diesem Modus werden nur die SYN-(TCP)-Pakete zurückgewiesen, die speziell die Quell-IP-Adresse behandeln.

   Logging: SYN-(TCP)-Flood-Attacken können dazu führen, dass sehr umfangreiche Protokolle erstellt werden. Mit diesem Drop-down-Menü können Sie den Umfang des Logging einstellen. Die möglichen Einstellungen sind **Alles** (**Everthing**), **Limitiert** (**Limited**) und **Aus** (**Off**).

4. Mit den folgenden beiden Einstellungen können Sie Netzwerke von der Funktion Portscan Detection auschließen.

   Skip Source Networks: Hier können Sie zuverlässige Quellnetzwerke auswählen, die von der Funktion ausgeschlossen werden sollen.

Skip Destination Networks: Hier können Sie zuverlässige Zielnetzwerke auswählen, die von der Funktion ausgeschlossen werden sollen.

5. Definieren Sie in den folgenden beiden Einstellungen die maximale Rate für die Datenpakete.

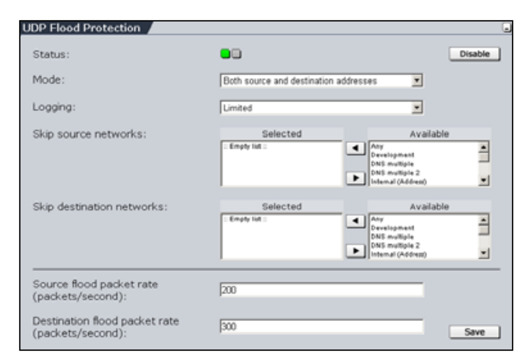
   Es ist sehr wichtig, dass Sie in den Eingabefeldern angemessene Werte eintragen. Wenn Sie die Werte zu hoch definieren, kann es passieren, dass z. B. Ihr Web-Server in die Knie geht, da er so eine große Summe an SYN-Paketen nicht bewältigen kann. Wenn auf der anderen Seite die Rate zu gering definiert wurde, kann es passieren, dass das Sicherheitssystem unvorhersehbar reagiert und reguläre Anfragen blockiert. Die Werte hängen hauptsächlich von der Hardware ab, auf der das Sicherheitssystem installiert ist. Ersetzen Sie daher die Standardeinstellungen durch für Ihr Sicherheitssystem geeignete Werte.

   Source flood packet rate (packets/second): Tragen Sie in das Eingabefeld die maximale Anzahl der Datenpakete pro Sekunde ein, die für Quell-IP-Adressen erlaubt sind.

   Destination flood packet rate (packets/second): Tragen Sie in das Eingabefeld die maximale Anzahl der Datenpakete pro Sekunde ein, die für Ziel-IP-Adressen erlaubt sind.

6. Speichern Sie die Einstellungen durch einen Klick auf die Schaltfläche **Save**.

UDP Flood Protection



Durch die Funktion **UDP Flood Protection** wird die Anzahl der UDP-Pakete, die in das lokale Netzwerk gesendet werden, begrenzt. Per Default ist die Funktion ausgeschaltet (Statusampel zeigt Rot).

UDP Flood Protection:

1. Öffnen Sie im Verzeichnis **Intrusion Protection** das Menü **DoS Flood Protection**.

2. Schalten Sie die Funktion durch einem Klick auf die Schaltfläche **Enable** bei **Status** ein.

   Anschließend öffnet sich ein erweitertes Eingabefenster.

3. Wählen Sie im Drop-down-Menü **Mode** den Modus aus.

   Both source and destination addresses: In diesem Modus werden UDP-Pakete zurückgewiesen, die sowohl die Quell-IP-adresse als auch die Ziel-IP-Adresse behandeln: zuerst werden die UDP-Pakete für die Quelladresse gefilter. Wenn dann noch zu viele Anfragen vorhanden sind, werden zusätzlich die UDP-Pakete für die Zieladresse gefiltert.

   Destination address only: In diesem Modus werden nur die UDP-Pakete zurückgewiesen, die speziell die Ziel-IP-Adresse behandeln.

   Source address only: In diesem Modus werden nur die UDP-Pakete zurückgewiesen, die speziell die Quell-IP-Adresse behandeln.

Logging: UDP-Flood-Attacken können dazu führen, dass sehr umfangreiche Protokolle erstellt werden. Mit diesem Drop-down-Menü können Sie den Umfang des Logging einstellen. Die möglichen Einstellungen sind **Alles** (**Everthing**), **Limitiert** (**Limited**) und **Aus** (**Off**).

4. Mit den folgenden beiden Einstellungen können Sie Netzwerke von der Funktion Portscan Detection auschließen.

   Skip Source Networks: Hier können Sie zuverlässige Quellnetzwerke auswählen, die von der Funktion ausgeschlossen werden sollen.

   Skip Destination Networks: Hier können Sie zuverlässige Zielnetzwerke auswählen, die von der Funktion ausgeschlossen werden sollen.

5. Definieren Sie in den folgenden beiden Einstellungen die maximale Rate für die Datenpakete.

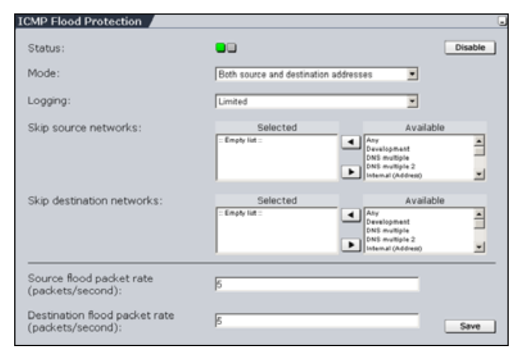
   Es ist sehr wichtig, dass Sie in den Eingabefeldern angemessene Werte eintragen. Wenn Sie die Werte zu hoch definieren, kann es passieren, dass Systeme in die Knie geht, da sie so eine große Summe an UDP-Paketen nicht bewältigen können. Wenn auf der anderen Seite die Rate zu gering definiert wurde, kann es passieren, dass das Sicherheitssystem unvorhersehbar reagiert und reguläre Anfragen blockiert. Die Werte hängen hauptsächlich von der Hardware ab, auf der das Sicherheitssystem installiert ist. Ersetzen Sie daher die Standardeinstellungen durch für Ihr Sicherheitssystem geiegnete Werte.

   Source flood packet rate (packets/second): Tragen Sie in das Eingabefeld die maximale Anzahl der Datenpakete pro Sekunde ein, die für Quell-IP-Adressen erlaubt sind.

   Destination flood packet rate (packets/second): Tragen Sie in das Eingabefeld die maximale Anzahl der Datenpakete pro Sekunde ein, die für Ziel-IP-Adressen erlaubt sind.

6. Speichern Sie die Einstellungen durch einen Klick auf die Schaltfläche **Save**.

ICMP Flood Protection



Durch die Funktion **ICMP Flood Protection** wird die Anzahl der ICMP-Pakete, die in das lokale Netzwerk gesendet werden, begrenzt. Per Default ist die Funktion ausgeschaltet (Statusampel zeigt Rot).

ICMP Flood Protection:

1. Öffnen Sie im Verzeichnis **Intrusion Protection** das Menü **DoS Flood Protection**.

2. Schalten Sie die Funktion durch einem Klick auf die Schaltfläche **Enable** bei **Status** ein.

   Anschließend öffnet sich ein erweitertes Eingabefenster.

3. Wählen Sie im Drop-down-Menü **Mode** den Modus aus.

   Both source and destination addresses: In diesem Modus werden ICMP-Pakete zurückgewiesen, die sowohl die Quell-IP-adresse als auch die Ziel-IP-Adresse behandeln: zuerst werden die UDP-Pakete für die Quelladresse gefilter. Wenn dann noch zu viele Anfragen vorhanden sind, werden zusätzlich die UDP-Pakete für die Zieladresse gefiltert.

   Destination address only: In diesem Modus werden nur die UDP-Pakete zurückgewiesen, die speziell die Ziel-IP-Adresse behandeln.

Source address only: In diesem Modus werden nur die UDP-Pakete zurückgewiesen, die speziell die Quell-IP-Adresse behandeln.

Logging: ICMP-Flood-Attacken können dazu führen, dass sehr umfangreiche Protokolle erstellt werden. Mit diesem Drop-down-Menü können Sie den Umfang des Logging einstellen. Die möglichen Einstellungen sind **Alles** (**Everthing**), **Limitiert** (**Limited**) und **Aus** (**Off**).

4. Mit den folgenden beiden Einstellungen können Sie Netzwerke von der Funktion Portscan Detection auschließen.

Skip Source Networks: Hier können Sie zuverlässige Quellnetzwerke auswählen, die von der Funktion ausgeschlossen werden sollen.

Skip Destination Networks: Hier können Sie zuverlässige Zielnetzwerke auswählen, die von der Funktion ausgeschlossen werden sollen.

5. Definieren Sie in den folgenden beiden Einstellungen die maximale Rate für die Datenpakete.

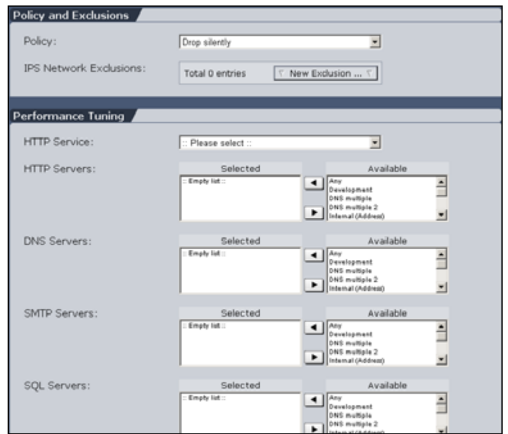
Es ist sehr wichtig, dass Sie in den Eingabefeldern angemessene Werte eintragen. Wenn Sie die Werte zu hoch definieren, kann es passieren, dass Systeme in die Knie geht, da sie so eine große Summe an ICMP-Paketen nicht bewältigen können. Wenn auf der anderen Seite die Rate zu gering definiert wurde, kann es passieren, dass das Sicherheitssystem unvorhersehbar reagiert und reguläre Anfragen blockiert. Die Werte hängen hauptsächlich von der Hardware ab, auf der das Sicherheitssystem installiert ist. Ersetzen Sie daher die Standardeinstellungen durch für Ihr Sicherheitssystem geiegnete Werte.

Source flood packet rate (packets/second): Tragen Sie in das Eingabefeld die maximale Anzahl der Datenpakete pro Sekunde ein, die für Quell-IP-Adressen erlaubt sind.

Destination flood packet rate (packets/second): Tragen Sie in das Eingabefeld die maximale Anzahl der Datenpakete pro Sekunde ein, die für Ziel-IP-Adressen erlaubt sind.

6. Speichern Sie die Einstellungen durch einen Klick auf die Schaltfläche **Save**.

5.4.5. Advanced



In diesem Menü können Sie für das Modul **Intrusion Protection System (IPS)** zusätzliche Einstellungen durchführen. Diese sollten aber nur von erfahrenen Benutzern vorgenommen werden.

Policy and Exclusions

Policy: Stellen Sie in diesem Drop-down-Menü ein, welche Sicherheitspolitik das Intrusion Protection System anwenden soll, wenn eine Blockierungsregel eine IPS-Angriffssignatur erkennt.

- **Drop silently**: Das Datenpaket wird nur blockiert.
- **Terminate connection**: An beide Kommunikationspartner wird ein TCP Reset, bzw. ein ICMP Port Unreachable (für UDP) abgeschickt und die Verbindung wird daraufhin beendet.

IPS Network Exclusions: In diesem Auswahlmenü können bestimmte Verbindungen zwischen den Netzwerken vom Intrusion Protection System (IPS) ausgeschlossen werden.

Die Verbindungen werden in einer Tabelle unter dem Auswahlmenü aufgelistet. Durch einen Klick auf das Papierkorp-Symbol () wird die definierte Verbindung wieder aus der Tabelle gelöscht.

Performance Tuning

Mit den Einstellungen in diesem Fenster kann die Leistung des *Intrusion Prevention System (IPS)* verbessert werden, indem die Server und Ports definiert werden. Die entsprechenden IPS-Regeln werden dann nur bei den eingestellten Servern und Ports angewendet.

Die Server müssen zuvor als Host im Menü **Definitions/Networks** hinzugefügt werden. Das Hinzufügen von Hosts wird in Kapitel 5.2.1 ab Seite 134 beschrieben.

Hinweis:

Wenn Sie in diesem Fenster keine Server einstellen, wird vom **Intrusion Protection System (IPS)** der gesamte Datenverkehr im gesamten Netzwerke gemäß den Einstellungen im Fenster **Global Settings** überwacht.

HTTP Service: Stellen Sie in diesem Drop-down-Menü den Zielport für den HTTP-Datenverkehr ein, indem Sie einen *Dienst* (*Service*) auswählen. Im Menü **Definitions/Services** können Sie falls erfoderlich den *Dienst* ändern oder einen neuen hinzufügen. Vom hinzugefügten Dienst wird nur die Zielportnummer verwendet. Bei einer Portrange wird nur der erste und der letzte Port verwendet.

Beispiel: Bei der Portrange 80:8080 wird die HTTP-Regel bei den Zielports 80 und 8080 angewendet.

HTTP Servers: Stellen Sie hier die HTTP-Server ein.

DNS Servers: Stellen Sie hier die DNS-Server ein.

SMTP Servers: Stellen Sie hier die SMTP-Server ein.

SQL Servers: Stellen Sie hier die SQL-Server ein.

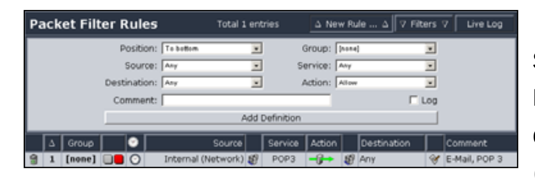
Telnet Servers: Stellen Sie hier die Telnet-Server ein.

5.5. Paketfilter (Packet Filter)

Der **Paketfilter (Packet Filter)** ist der zentrale Teil der Firewall. Im Menü **Rules** bestimmen Sie durch Setzen der **Paketfilterregeln**, welcher Datenverkehr zwischen den Netzwerken/Hosts erlaubt ist. Sie können außerdem festlegen, dass spezielle Pakete explizit gefiltert werden und die Firewall nicht passieren dürfen. Das Paketfiltermanagement erfolgt über die **Regelsatztabelle**.

Mit den Werkzeugen im Menü **ICMP** können die Netzwerkverbindungen und die Funktionalität des Internet-Sicherheitssystems getestet werden und im Menü **Advanced** befinden sich die Zusatz- und Reporting-Funktionen.

5.5.1. Rules



Im Menü **Rules** verwalten Sie das Paketfilterregelwerk. Die Regeln werden mit Hilfe der definierten Netzwerke (**Networks**) und Dienste (**Services**) gesetzt.

Beim Einsatz von Paketfiltern unterscheidet man zwei grundlegende Arten der Security Policy:

- Alle Pakete passieren – dem Regelwerk muss ausdrücklich mitgeteilt werden, was verboten ist.
- Alle Pakete werden geblockt – das Regelwerk braucht Informationen, welche Pakete passieren dürfen.

Die Firewall dieses Internet-Sicherheitssystems ist fest auf die Variante **Alle Pakete werden geblockt** voreingestellt, da mit diesem Vorgehen eine viel höhere Sicherheit erreicht werden kann. Für den täglichen Umgang bedeutet dies, dass Sie ausdrücklich definieren, welche IP-Pakete den Filter passieren dürfen. Alle übrigen Pakete werden geblockt und anschließend im **Packet Filter Live Log** angezeigt. Das

Packet Filter Live Log kann in diesem Menü durch einen Klick auf die Schaltfläche **Live Log** oder im Menü **Packet Filter/Advanced** geöffnet werden. Die Funktionen im **Packet Filter Live Log** werden in Kapitel 5.5.3 ab Seite 260 beschrieben.

Beispiel:

Netzwerk A ist ein Sub-Netzwerk von Netzwerk B. In Regel 1 wird der Dienst SMTP für das Netzwerk A erlaubt. Regel 2 verbietet SMTP für das Netzwerk B.
Ergebnis: Ausschließlich für Netzwerk A wird SMTP erlaubt. SMTP-Pakete von allen anderen IP-Adressen aus dem restlichen Netzwerk B dürfen nicht passieren.

Eine Paketfilterregel setzt sich aus der **Quelladresse** (**Source**), einem **Dienst** (**Service**), einer **Zieladresse** (**Destination**) und einer **Maßnahme** (**Action**) zusammen.

Als Quell- und Zieladresse können die folgenden Werte ausgewählt werden. Die Funktionen werden in den Kapiteln zu den entsprechenden Menüs erklärt:

- Ein Netzwerk (**Network**) - die Netzwerke werden im Menü **Definitions/Networks** definiert.
- Eine **Netzwerkgruppe** (**Network Group**) - die Netzwerkgruppen werden im Menü **Definitions/Networks** definiert.
- Ein **Schnittstellen-Netzwerk** (**Interface**) - diese logischen Netzwerke werden beim Konfigurieren der Netzwerkkarten und Schnittstellen vom System automatisch definiert. Die Schnittstellen werden im Menü **Network/Interfaces** konfiguriert.
- Ein **IPSec Remote Key Object** (**IPSec User Group**) – die IPSec-Benutzergruppen werden im Menü **Definitions/Networks** definiert. Diese Adresse oder Portrange benötigen Sie, wenn Sie Paketfilterregeln für IPSec-Road Warrior-Endpunkte setzen möchten.

Eine neu definierte Paketfilterregel wird zunächst deaktiviert in die Tabelle eingetragen. Die aktivierten Paketfilterregeln werden der Reihe nach von der Firewall abgearbeitet bis eine Regel zutrifft. Die Reihenfolge der Abarbeitung wird in der Tabelle durch die **Positionsnummer** (zweite Spalte von links) angezeigt. Falls Sie die Tabelle später sortieren, z. B. nach der *Quelladresse* (*Source*), beachten Sie bitte, dass die Anzeige der Regeln nicht mehr mit der Reihenfolge der Regelabarbeitung übereinstimmt. Falls Sie allerdings die Reihenfolge der Regeln über die **Positionsnummer** verändern, wird auch die Reihenfolge der Abarbeitung verändert. Falls im vorangehenden Beispiel die Regel 2 vor die Regel 1 verschoben wird, ist der Dienst SMTP für beide Netzwerke nicht mehr erlaubt. Seien Sie sehr gewissenhaft bei der Definition dieses Regelsatzes, er bestimmt die Sicherheit der Firewall.

Wichtiger Hinweis:

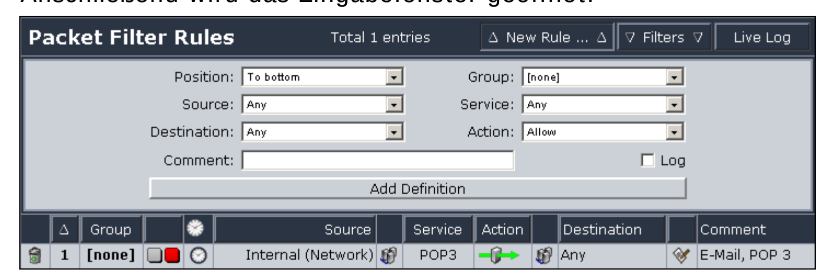
Wenn eine Regel zutrifft, werden die nachfolgenden Regeln nicht mehr beachtet! Die Reihenfolge ist daher sehr wichtig. Setzen Sie nie eine Regel mit den Einträgen **Any** (*Source*) – **Any** (*Service*) – **Any** (*Destination*) – **Allow** (*Action*) an die Spitze Ihres Regelwerks.

Paketfilterregel setzen:

1. Öffnen Sie im Verzeichnis **Packet Filter** das Menü **Rules**.

2. Klicken Sie auf die Schaltfläche **New Rule**.

   Anschließend wird das Eingabefenster geöffnet.



3. Führen Sie die folgenden Einstellungen durch:

Position: Bestimmen Sie, in welche Zeile der Tabelle die Paketfilterregel eingefügt werden soll. Die Reihenfolge der Paketfilterregeln kann auch später geändert werden. Per Default wird die Regel an das Ende (**To Bottom**) der Regeltabelle eingefügt.

Group: Zur einfacheren Administration des Regelwerks können die Paketfilterregeln einer Gruppe zugeteilt werden. Die Zugehörigkeit zu einer Gruppe hat keinen Einfluss auf die Abarbeitung der Regel im Regelwerk.
Bei der ersten Regel kann in diesem Drop-down-Menü noch keine Gruppe ausgewählt werden. Neue Gruppen werden in der Regelsatztabelle definiert.

Source: Wählen Sie im Drop-down-Menü die Quelladresse der Datenpakete aus. Die Einstellung **Any** trifft auf alle IP-Adressen zu, egal ob es sich um offiziell zugeteilte oder private IP-Adressen gemäß RFC1918 handelt.

Service: Wählen Sie im Drop-down-Menü den Dienst aus.

Im Drop-down-Menü sind sowohl die vordefinierten als auch die von Ihnen selbst festgelegten Dienste enthalten. Mit Hilfe dieser Dienste lässt sich der zu bearbeitende Datenverkehr präzise definieren. Die Einstellung **Any** steht hier stellvertretend für alle Kombinationen aus Protokollen und Quell- bzw. Zielport.

Destination: Wählen Sie im Drop-down-Menü die Zieladresse der Datenpakete aus. Die Einstellung **Any** trifft auf alle IP-Adressen zu, egal ob es sich um offiziell zugeteilte oder private IP-Adressen gemäß RFC1918 handelt.

Action: Wählen Sie im Drop-down-Menü die Aktion aus, die der Paketfilter ergreift, wenn ein Datenpaket den Einstellungen **Source**, **Service** und **Destination** entspricht. In Verbindung mit der Aktion wird hier auch die Priorität für die Funktion **Quality of Service (Qos)** eingestellt.

Wichtiger Hinweis:

Damit die Prioritäten (**high priority** und **low priority**) wirksam werden, müssen Sie im Menü **Network/Interfaces** die entsprechende Schnittstelle für die Funktion **QoS** aktivieren und die Werte **Uplink Bandwidth (kbits)** und **Downlink Bandwidth (kbits)** definieren.

Allow: Alle Pakete, die diese Bedingung erfüllen, werden durchgelassen.

Allow (high priority): Alle Pakete, die diese Bedingung erfüllen, werden durchgelassen. Zusätzlich erhält dieser Datenverkehr bei ausgelastetem Uplink eine höhere Priorität.

Allow (low priority): Alle Pakete, die diese Bedingung erfüllen, werden durchgelassen. Zusätzlich erhält dieser Datenverkehr bei ausgelastetem Uplink eine niedrigere Priorität.

Drop: Alle Pakete, die diese Bedingung erfüllen, werden blockiert.

Reject: Alle Pakete, die diese Bedingung erfüllen, werden abgewiesen. Der Absender erhält eine entsprechende ICMP-Nachricht.

Log: Die Regelverletzung wird im **Packet Filter Live Log** protokolliert. Die Aktion wird durch einen Klick auf das Kontrollkästchen eingeschaltet.

Bei Filterverletzungen, die dauernd stattfinden, sicherheitstechnisch nicht relevant sind und nur die Übersichtlichkeit des **Packet Filter Live Log** beeinträchtigen (z. B. Netbios-Broadcasts von MS-Windows-Rechnern) ist es empfehlenswert die Funktion **Log** nicht zu aktivieren.

Comment: Über das Eingabefeld können Sie optional einen Kommentar für die Regel hinzufügen.

4. Speichern Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add Definition**.

   Nach erfolgreicher Definition wird die neue **Paketfilterregel** immer deaktiviert in die Regelsatztabelle eingetragen (Statusampel zeigt Rot).



	Δ	Group			Source		Service	Action		Destination		Comment
	1	[none]			Internal (Network)		POP3			Any		E-Mail, POP 3

5. Aktivieren Sie die Paketfilterregel durch einen Klick auf die Statusampel.

Anschließend stehen Ihnen in der Regelsatztabelle zur Bearbeitung der Paketfilterregeln weitere Funktionen zur Verfügung.

Hinweis:

Neue Regeln werden per Default **deaktiviert** in die Regelsatztabelle eingefügt. Die Paketfilterregel wird erst wirksam, wenn sie von Ihnen aktiviert wird. Sehen Sie dazu **Regel aktivieren / deaktivieren**.

Die Regelsatztabelle

Jede Paketfilterregel wird in der Tabelle duch eine separate Zeile dargestellt: Die verschiedenen Einstellungen werden entweder durch alphanumerische Zeichen oder durch Symbole angezeigt. Während alle Einstellungen mit einer alphanummerischen Anzeige durch einen Klick auf das entsprechende Feld editiert werden können, ist dies nicht bei allen Symbol-Anzeigen möglich.



	Δ	Group			Source		Service	Action		Destination		Comment
	1	[none]			Internal (Network)		POP3			Any		E-Mail, POP 3

In der nachfolgenden Tabelle werden alle Symbole aus der Regelsatztabelle erklärt.

Die Symbole

Icon	Spalte	Anzeige / Einstellung
		Papierkorb
	Statusampel	Paketfilterregel ist deaktiviert
	Statusampel	Paketfilterregel ist aktiviert
	Uhr	Zeitgesteuertes Ereignis
	Source/Destination	Host
	Source/Destination	Netzwerk
	Source/Destination	Netzwerkgruppe
	Source/Destination	DNS Hostname
	Source/Destination	IPSec User Group
	Action	Allow
	Action	Allow (high priority)
	Action	Allow (low priority)
	Action	Drop
	Action	Reject
	Log	Protokoll (Log) ausgeschaltet
	Log	Protokoll (Log) eingeschaltet

Gruppe hinzufügen / editieren: Durch einen Klick auf das Feld in der Spalte **Group** wird ein Eingabefeld geöffnet. Mit einem Klick auf die Schaltfläche **Save** werden die Änderungen gespeichert.
Um den Vorgang abzubrechen klicken Sie auf die Schaltfläche **Cancel**.

Paketfilterregel aktivieren / deaktivieren: Die Statusampel in der vierten Spalte zeigt den Status der Paketfilteregel an. Mit einem Klick auf die Statusampel wird die Regel **aktiviert** (Statusampel zeigt

Grün) und **deaktiviert** (Statusampel zeigt Rot).
Deaktivierte Regeln bleiben gespeichert, werden aber vom Paketfilter nicht berücksichtigt.

Zeitsteuerung aktivieren: Durch einen Klick auf das Feld in der Spalte mit dem Uhren-Symbol () wird ein Dop-down-Menü geöffnet. Nun können Sie das Zeitintervall für die Paketfilterregel auswählen. Durch einen Klick auf die Schaltfläche **Save** werden die Änderungen gespeichert.
Um den Vorgang abzubrechen klicken Sie auf die Schaltfläche **Cancel**.

Wenn für eine Paketfilterregel ein Zeitintervall eingestellt ist, wird im entsprechenden Feld das Uhren-Symbol angezeigt. Die genauen Einstellungen für dieses Zeitintervall werden angezeigt, wenn Sie mit der Maus dieses Uhrensymbol berühren.

Die Zeitinterwalle werden im Menü **Definitions/Time Events** definiert. Das Menü wird in Kapitel 5.2.4 ab Seite 150 beschrieben.

Paketfilterregel editieren: Durch einen Klick auf die entsprechende Einstellung wird ein Eingabefeld geöffnet. Anschließend können Sie die Eingaben bearbeiten. Durch einen Klick auf die Schaltfläche **Save** werden die Änderungen gespeichert.
Um den Vorgang abzubrechen klicken Sie auf die Schaltfläche **Cancel**.

Reihenfolge der Paketfilterregel ändern: Die Abfolge der Paketfilterregeln in der Tabelle ist ausschlaggebend für das korrekte Funktionieren der Firewall. Durch einen Klick auf die Positionsnummer können Sie die Reihenfolge der Abarbeitung verändern. Wählen Sie im Drop-down-Menü die Position aus, wohin die Paketfilterregel verschoben werden soll und bestätigen Sie dies durch einen Klick auf die Schaltfläche **Save**.

Paketfilterregel löschen: Durch einen Klick auf das Papierkorb-Symbol wird die Paketfilterregel aus der Tabelle gelöscht.

Regelsatztabelle sortieren: Durch einen Klick auf die Funktion in der Kopfzeile der Regelsatz-Tabelle werden alle Regeln entsprechend sortiert. Wenn Sie z. B. die Tabelle nach den Absendernetzwerken

sortieren möchten, klicken Sie auf **Source**. Um die Tabelle wieder nach der Reihenfolge des **Matching** anzuzeigen, klicken Sie auf die Spalte mit den Positionsnummern.

Filters

Mit der Funktion **Filters** können Sie aus der Tabelle *Paketfilterregeln* (*Packet Filter Rules*) mit bestimmten Attributen herausfiltern. Diese Funktion erleichtert das Managen von großen Netzwerken mit einem umfangreichen Regelwerk, da Regeln eines bestimmten Typs übersichtlich dargestellt werden können.

Regeln filtern:

1. Klicken Sie auf die Schaltfläche **Filters**.

   Anschließend wird das Eingabefenster geöffnet.

2. Tragen Sie in den nachfolgend aufgeführten Feldern die Attribute für den Filter ein. Es müssen nicht alle Attribute definiert werden.

   Group: Falls Sie Regeln einer bestimmten Gruppe filtern möchten, wählen Sie diese im Drop-down-Menü aus.

   State: Mit diesem Drop-down-Menü filtern Sie Regeln mit einem bestimmten Status.

   Source: Mit diesem Drop-down-Menü filtern Sie Regeln mit einer bestimmten Quelladresse.

   Service: Falls Sie Regeln mit einem bestimmten Dienst filtern möchten, wählen Sie diesen im Drop-down-Menü aus.

   Action: Mit diesem Drop-down-Menü filtern Sie Regeln mit einer bestimmten Aktion.

   Destination Port: Mit diesem Drop-down-Menü filtern Sie Regeln mit einer bestimmten Zieldresse.

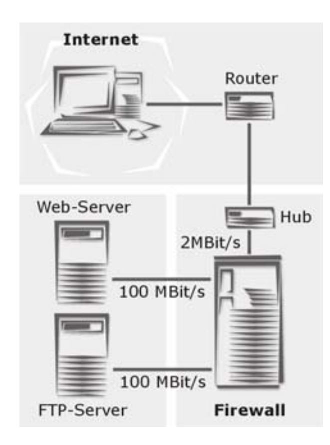
   Log: Mit diesem Drop-down-Menü filtern Sie Regeln die protokolliert werden.

Comment: Falls Sie Regeln mit bestimmten Kommentaren filtern möchten, tragen Sie die Begriffe in das Eingabemenü ein.

3. Um den Filter zu starten klicken Sie auf die Schaltfläche **Apply Filters**.

Ansschließend werden nur die gefilterteten Paketfilterregeln in der Tabelle angezeigt. Nach Verlassen des Menüs wird wieder das vollständige Regelwerk dargestellt.

Quality of Service (QoS)



Die Übertragungsleistung eines Leitungssystems wird als Bandbreite bezeichnet und wird hier in kBit/s angegeben. Falls die anfallende Datenmenge die Leistungsgrenze überschreitet, kann die Kommunikation entweder sehr langsam werden oder sogar gänzlich zusammenbrechen.

In der linken Grafik ist z. B. ein Netzwerk mit einem Web-Server und einem FTP-Server dargestellt. Beide Server teilen sich eine 2 MBit-Leitung zum Internet. Protokollbedingt nutzen TCP-basierende Aplikationen (z. B. FTP) immer die volle Bandbreite. Dies kann zur Folge haben, dass für den Web-Server nicht mehr genug Bandbreite zur Verfügung steht.

Mit der **Quality-of-Service-(QoS)**-Funktionalität können Sie den Verbindungen für den Fall eines ausgelasteten Uplinks verschiedene Prioritäten zuordnen. Diese Prioritäten werden in den Paketfilteregeln durch die Aktionen **Allow**, **Allow (high priority)** und **Allow (low priority)** definiert.

Wichtiger Hinweis:

Damit die Prioritäten (**high priority** und **low priority**) wirksam werden, müssen Sie im Menü **Network/Interfaces** auf der entsprechenden Schnittstelle die Funktion **QoS** einschalten und die Werte **Uplink Bandwidth** und **Downlink Bandwidth** definieren.

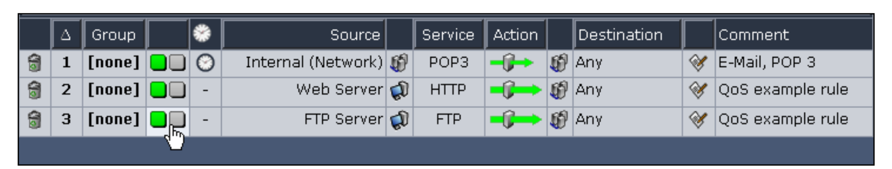
Damit die Verbindung vom Web-Server, wie in dem Beispiel dargestellt, die gleiche Bandbreite erhält wie die Verbindung vom FTP-Server ist nur zu Beachten, dass bei beiden Paketfilterregeln die gleiche **Aktion** (**Action**) eingestellt wird:

1. Paketfilterregel für Datenpakete vom Web-Server:

Source: Web-Server
Service: HTTP
To (Server): Internet
Action: Allow (high priority)

2. Paketfilterregel für Datenpakete vom FTP-Server:

Source: FTP-Server
Service: FTP
Destination: Internet
Action: Allow (high priority)



	Δ	Group			Source		Service	Action		Destination		Comment
	1	[none]			Internal (Network)		POP3			Any		E-Mail, POP 3
	2	[none]		-	Web Server		HTTP			Any		QoS example rule
	3	[none]		-	FTP Server		FTP			Any		QoS example rule

Wenn der Uplink nur von den Datenpaketen der beiden Server verwendet wird, erhält im **Worst Case** jede Verbindung die Hälfte der Bandbreite (1MBit/s). Die Einstellung **High Priority** wird erst relevant, wenn eine dritte Datenverbindung aufgebaut wird. Alle Verbindungen mit einer niedrigeren Priorität, **Allow** oder **Allow (low priority)**, werden nachrangig behandelt.

Weitere Funtionen und Einstellungen

Broadcast auf das gesamte Internet:

Um Pakete mit der Zieladresse **Broadcast-IP** zu **droppen**, müssen Sie zuerst im Menü **Definitions/Networks** die entsprechende Broadcast-Adresse in Form eines neuen Netzwerks definieren. Anschließend müssen Sie die Paketfilterregel setzen und aktivieren.

1. Öffnen Sie im Verzeichnis **Definitions** das Menü **Networks** und definieren Sie das folgende Netzwerk:

   Name: Broadcast32

   Type: Host

   IP Address: 255.255.255.255

   Comment (optional): Tragen Sie einen Kommentar ein.

2. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add Definition**.

3. Öffnen Sie nun im Verzeichnis **Packet Filter** das Menü **Rules** und setzen Sie die folgende Paketfilterregel:

   Source: Any

   Service: Any

   Destination: Broadcast32

   Action: Drop

   Comment (optional): Tragen Sie einen Kommentar ein.

4. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add Definition**.

Broadcast auf ein Netzwerksegment:

Für jede im Menü **Interfaces** konfigurierte Schnittstelle wird automatisch das Netzwerk **NAME (Broadcast)** definiert.
Weitere Informationen hierzu erhalten Sie in Kapitel 5.3.2 ab Seite 154 unter der Überschrift **Current Interface Status**.

1. Öffnen Sie im Verzeichnis **Packet Filter** das Menü **Rules** und setzen Sie die folgende Paketfilterregel:

   Source: Any

   Service: Any

   Destination: Wählen Sie hier das Netzwerk Broadcast des entsprechenden Netzwerksegments aus.
   Beispiel: NAME (Broadcast)

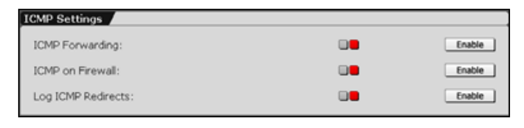
   Action: Drop

   Comment (optional): Tragen Sie einen Kommentar ein.

2. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add Definition**.

5.5.2. ICMP

ICMP Settings



In diesem Fenster werden die Einstellungen für das **Internet Control Message Protocol (ICMP)** vorgenommen. **ICMP** ist notwendig, um die Netzwerkverbindungen und Funktionalität des Internet-Sicherheitssystems zu testen. Des Weiteren wird *ICMP* zur Fehlerbenachrichtigung und zu Diagnosezwecken verwendet.

Hinweis:

Nähere Informationen zu **ICMP** finden Sie auch unter **Ping** und **Traceroute**.

ICMP on Firewall und **ICMP Forwarding** beziehen sich immer auf alle IP-Adressen (**Any**). Wenn diese Funktionen eingeschaltet sind (Statusampel zeigt Grün), können alle IPs die Firewall (**ICMP on Firewall**) bzw. das Netzwerk dahinter (**ICMP Forwarding**) anpingen. Einzelne IP-Adressen können dann nicht mehr mit Paketfilterregeln ausgeklammert werden.

Wichtiger Hinweis:

Die hier getroffenen Einstellungen haben stets Priorität gegenüber den Einstellungen, die im Paketfilterregelsatz definiert sind.

Wenn die **ICMP**-Einstellungen ausgeschaltet sind (Statusampel zeigt Rot), kann man mit geeigneten Paketfilterregeln einzelnen IPs und Netzwerken das Senden von ICMP-Paketen auf die Firewall bzw. durch die Firewall erlauben.

ICMP Forwarding: Alle ICMP-Pakete werden hinter die Firewall weitergeleitet. Dies bedeutet, dass alle IPs im lokalen Netzwerk und in allen angeschlossenen DMZs angepingt werden können.
Mit einem Klick auf die Schaltfläche **Enable** schalten Sie die Funktion ein (Statusampel zeigt Grün).

Wichtiger Hinweis:

Falls Sie **ICMP Forwarding** ausschalten möchten, darf im Menü **Packet Filter/Rules** keine Regel mit den Einträgen **Any** (*Source*) – **Any** (*Service*) – **Any** (*Destination*) – **Allow** (*Action*) definiert sein. Das **ICMP Forwarding** bleibt sonst aktiv.

ICMP on Firewall: Die Firewall empfängt und sendet direkt alle ICMP-Pakete. Per Default ist diese Funktion eingeschaltet (Statusampel zeigt Grün).
Mit einem Klick auf die Schaltfläche **Disable** schalten Sie die Funktion aus (Statusampel zeigt Rot).

Hinweis:

Für die Aktion **Ping** muss hier die Funktion **ICMP on Firewall** eingeschaltet sein. Die Aktion befindet sich im Menü **Network/Ping Check** und wird in Kapitel 5.3.9 ab Seite 221 beschrieben.

Log ICMP Redirects: Die **ICMP Redirects** werden von Routern gegenseitig verschickt, um eine bessere Route zu einem Ziel zu finden. Router ändern daraufhin ihre Routing-Tabellen und leiten die folgenden Pakete zum gleichen Ziel auf der vermeintlich besseren Route weiter.
Mit dieser Funktion werden die *ICMP Redirects* protokolliert. Mit einem Klick auf die Schaltfläche **Enable** schalten Sie die Funktion ein (Statusampel zeigt Grün).

Hinweis:

Falls die Firewall im **ICSA Labs Compliant Mode** arbeitet, schalten Sie diese Funktion nicht aus. Weitere Informationen zum *Common Criteria Mode* erhalten Sie in Kapitel 5.1.12 auf Seite 129.

Traceroute Settings



Traceroute ist ein Werkzeug, um Fehler beim Routing in Netzwerken zu finden. Mit diesem Tool kann der Weg zu einer IP-Adresse aufgelöst werden. Traceroute listet die IP-Adressen der Router auf, über die das versendete Paket transportiert wurde. Sollte der Pfad der Datenpakete kurzfristig nicht nachweisbar sein, wird die Unterbrechung durch Sterne (*) angezeigt. Nach einer bestimmten Menge an Unterbrechungen wird der Versuch abgebrochen. Die Verbindungsunterbrechung kann viele Gründe haben, z. B. auch, dass ein Paketfilter im Netzwerkpfad kein Traceroute erlaubt.

In diesem Fenster werden die erweiterten Einstellungen speziell für **ICMP Traceroute** vorgenommen. Zusätzlich werden die UDP-Ports für **UNIX Traceroute**-Anwendungen geöffnet.

Firewall is Traceroute visible: Die Firewall antwortet auf **Traceroute**-Pakete. Mit einem Klick auf die Schaltfläche **Enable** schalten Sie die Funktion ein (Statusampel zeigt Grün).

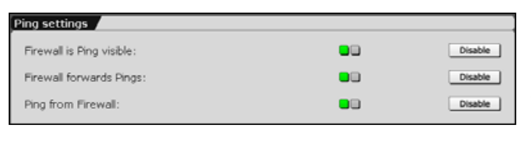
Firewall forwards Traceroute: Die Firewall leitet **Traceroute**-Pakete weiter.
Mit einem Klick auf die Schaltfläche **Enable** schalten Sie die Funktion ein (Statusampel zeigt Grün).

Hinweis:

Die Funktionen **Firewall is Traceroute visible** und **Firewall forwards Traceroute** machen nur Sinn, wenn beide eingeschaltet sind.

Traceroute from Firewall: Der Traceroute-Befehl kann auf der Firewall verwendet werden.
Mit einem Klick auf die Schaltfläche **Enable** schalten Sie die Funktion ein (Statusampel zeigt Grün).

Ping Settings



Hier werden die erweiterten Einstellungen speziell für **ICMP Ping** vorgenommen.

Weitere Informationen zu **Ping** erhalten Sie im Kapitel 5.3.9 ab Seite 221.

Firewall is Ping visible: Die Firewall antwortet auf **Ping**-Pakete.
Mit einem Klick auf die Schaltfläche **Enable** schalten Sie die Funktion ein (Statusampel zeigt Grün).

Hinweis:

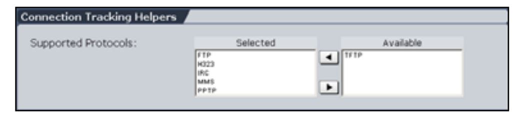
Falls die Firewall im **ICSA Labs Compliant Mode** arbeitet, schalten Sie diese Funktion nicht ein. Weitere Informationen zum *ICSA Labs Compliant Mode* erhalten Sie in Kapitel 5.1.12 auf Seite 129.

Firewall forwards Ping: Die Firewall leitet **Ping**-Pakete weiter.
Mit einem Klick auf die Schaltfläche **Enable** schalten Sie die Funktion ein (Statusampel zeigt Grün).

Ping from Firewall: Der **Ping**-Befehl kann auf der Firewall verwendet werden. Mit einem Klick auf die Schaltfläche **Enable** schalten Sie die Funktion ein (Statusampel zeigt Grün).

5.5.3. Advanced

Connection Tracking Helpers



Der **Stateful Inspection Packet Filter** und die **NAT**-Funktionalität werden durch das Modul *iptables* im Sub-System *Netfilter* bereitgestellt. Alle Verbindungen, die über den Paketfilter betrieben werden, werden durch das Modul *Conntrack* mitverfolgt: dies bezeichnet man als **Connection Tracking**.

Einige Protokolle, wie FTP oder IRC benötigen mehrere Kommunikationskanäle und diese können nicht über Portnummern miteinander in Verbindung gebracht werden. Damit nun diese Protokolle über den *Paketfilter* betrieben werden können, bzw. eine Adressumsetzung durch *NAT* erfolgen kann werden die **Connection Tracking Helpers** benötigt. Helpers sind Strukturen, die auf sogenannte Conntrack-Helper verweisen. Dies sind in der Regel zusätzliche Kernel-Module, die dem Modul Conntrack helfen bestehende Verbindungen zu erkennen.

Für FTP-Datenverbindungen wird z. B. ein FTPConntrack-Helper benötigt. Dieser erkennt die zur Kontrollverbindung (normalerweise TCP Port 21) gehörenden Datenverbindungen, deren Zielport beliebig sein kann, und fügt entsprechende expect-Strukturen zur expect-Liste hinzu.

Die folgenden Protokolle werden unterstützt:

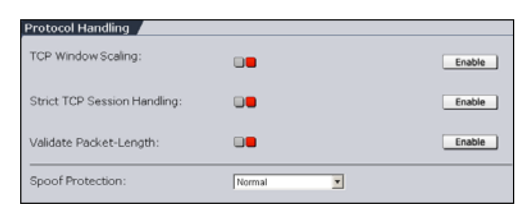
- FTP (File Transfer Protocol)
- H323
- IRC (für DCC)
- MMS (Microsoft Media Streaming)
- PPTP (Point to Point Tunneling Protocol)

- TFTP (Trivial File Transport Protocol)

Helper-Module laden: Per Default sind alle Helper-Module mit der Ausnahme von TFTP geladen.
Das Laden und Entfernen der Helper-Module erfolgt über das Auswahlfeld.

Die Funktionsweise des **Auswahlfeldes** wird in Kapitel 4.3.2 ab Seite 41 beschrieben.

Protocol Handling



TCP Window Scaling: Jedes TCP-Paket enthält im Header ein Window-Feld. Im Window wird definiert (in Bytes), welche Datenmenge ein System, das entsprechende Pakete verschickt von der Gegenstelle wiederum empfangen kann. Das Window ist eine Art Datenflusskontrolle, die verhindern soll, dass eine Gegenstelle mit Daten überflutet wird. Das TCP-Window-Feld hat eine Weite von 16 Bits und ermöglicht eine maximale Window-Größe von 64 kB.
Bei Netzwerken mit höherer Bandbreite sollte allerdings ein größeres TCP Window verwendet werden. Beim Window Scaling wird eine TCP-Variante eingesetzt, die einen höheren Skalierfaktor enthält. Dadurch kann das Window bis auf eine Größe zwischen 64 kB und 1 GB erweitert werden. Die Funktion TCP Window Scaling kann nur genutzt werden, wenn die Gegenstelle diese Funktion ebenfalls unterstützt.

Strict TCP Session Handling: Um einen zuverlässigen Datentransport zu gewährleisten, wird das in der Transportschicht vorhandene Transmission Control Protocol (TCP) verwendet. TCP baut dabei eine Rechner- zu Rechnerverbindung auf und sendet Daten solange erneut ab, bis es vom Zielrechner eine positive Bestätigung über den Erhalt der Daten empfängt. Dieser Verbindungsaufbau wird als **TCP Hand-**

shake bezeichnet und erfolgt in drei Schritten. Bevor ein Client z. B. mit einem Server Daten austauschen kann, sendet er zuerst ein TCP-Paket, in dessen Header unter anderem das sogenannte SYN-Bit (Sequenznummer) gesetzt ist. Dieses ist eine Aufforderung an den Server, eine Verbindung herzustellen. Außerdem übermittelt der Client die sogenannte Fenstergröße. Dieser Wert legt die maximale Anzahl der Byte für die Nutzdaten im Datenpaket fest, damit dieses auf dem Client noch verarbeitet werden kann. Im zweiten Schritt antwortet der Server, in dem er sein ACK-Bit (Acknowledge) im Header setzt und übermittelt ebenfalls seine Fenstergröße. Im letzten Schritt akzeptiert der Client mit dem ACK-Bit und beginnt anschließend mit dem Senden der eigentlichen Daten.
Die Firewall nimmt PSH-Pakete an ohne, dass sie einen **TCP Handshake** erhalten hat. Dies ist z. B. notwendig, wenn nach einem **Restart** des Internet-Sicherheitssystems oder nach einer Übernahme des zweiten Firewall-Systems bei einem **High-Availability**-System die bestehenden Verbindungen nicht verloren gehen soll.

Wenn die Funktion **Strict TCP Session Handling** eingeschaltet ist, erfolgt der Verbindungsaufbau mittels **TCP Handshake**.

Hinweis:

Falls die Firewall im **Common Criteria Mode** oder **ICSA Labs Compliant Mode** arbeitet, schalten Sie diese Funktion nicht aus. Weitere Informationen zum *Common Criteria Mode* und *ICSA Labs Compliant Mode* erhalten Sie in Kapitel 5.1.12 auf Seite 129.

Validate Packet-Length: Der **Paketfilter** (**Packet Filter**) prüft die Datenpakete auf die minimale Länge wenn das Protokoll icmp, tcp oder udp verwendet wird.

Die minimalen Datenlängen für die einzelnen Protokolle sind:

- icmp: 22 bytes
- tcp: 48 bytes

- udp: 28 bytes

Wenn die Datenpakete kürzer als die Minimalwerte sind, werden diese blockiert und in der Log-Datei **Packet Filter** mit dem Vermerk **INVALID_PKT:** protokolliert.
Die Log-Dateien werden im Menü **Local Logs/Browse** verwaltet.

Hinweis:

Falls die Firewall im **Common Criteria Mode** oder **ICSA Labs Compliant Mode** arbeitet, schalten Sie diese Funktion nicht aus. Weitere Informationen zum *Common Criteria Mode* und *ICSA Labs Compliant Mode* erhalten Sie in Kapitel 5.1.12 auf Seite 129.

Spoofing Protection: IP Spoofing ist ein Angriff, bei dem Pakete mit einer gefälschten Absenderadresse (Source IP) verschickt werden. Auf diese Weise sollen Authentifizierungs- und Identifikationsverfahren umgangen werden, die auf der Verwendung vertrauenswürdiger IP-Adressen oder Hostnamen beruhen. Viele der *Exploits* im Internet, die *Teardrop-* oder *Ping-of-Death*-Angriffe ausführen verwenden dieses Spoofing.

Spoof Protection vergleicht abhängig von der ausgewählten Einstellung nach bestimmten Verfahren die Absenderadresse des ankommenden Datenpakets mit den IPs der beteiligten Schnittstellen.

Die folgenden Einstellungen stehen zur Verfügung:

Normal: Das Sicherheitssystem fängt und protokolliert alle Datenpakete, die als Absenderadresse (Source IP) entweder die gleiche IP enthalten, wie die eigene Schnittstelle auf der die Pakete eintreffen oder wenn die Absenderadresse mit der IP eines Netzwerks übereinstimmt die einer der anderen Schnittstellen auf dem Sicherheitssystem zugewiesen ist.

Strict: Mit dieser Einstellung werden alle Datenpakete abgefangen, die zwar die richtige Zieladresse (Destination IP) für eine bestimmte Schnittstelle im Netzwerk enthalten, allerdings über eine Schnittstelle

der sie nicht zugeordnet sind im Netzwerk eintreffen.
Des Weiteren werden alle Pakete abgefangen, die von einer externen IP direkt an eine interne IP gesendet werden, da eigentlich vorausgesetzt wird, dass sie nur Datenpakete von internen Absenderadressen empfangen kann.

Hinweis:

Falls die Firewall im **Common Criteria Mode** oder **ICSA Labs Compliant Mode** arbeitet, behalten Sie die Einstellung **Strict** bei. Weitere Informationen zum *Common Criteria Mode* und *ICSA Labs Compliant Mode* erhalten Sie in Kapitel 5.1.12 auf Seite 129.

Logging Options



Log Unique DNS Requests: DNS-Pakete, die an oder durch die Firewall geschickt werden, und eine DNS-Anfrage enthalten werden in der Log-Datei **Packet Filter** mit dem Vermerk **DNS_REQUEST:** protokolliert.
Die Log-Dateien werden im Menü **Local Logs/Browse** verwaltet.

Log FTP Data Connections: Alle FTP-Datenverbindungen – ob im **Active** oder im **Passive Mode** - werden in der Log-Datei **Packet Filter** mit dem Vermerk **FTP_DATA:** protokolliert.
Die Log-Dateien werden im Menü **Local Logs/Browse** verwaltet.

Hinweis:

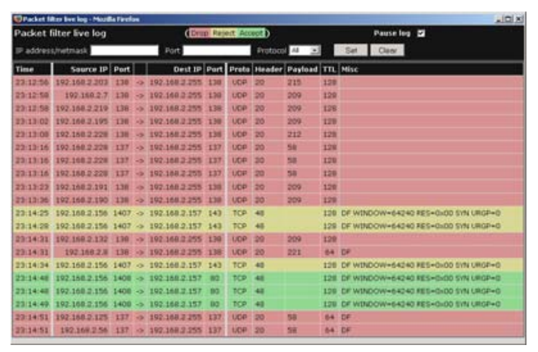
Falls die Firewall im **ICSA Labs Compliant Mode** arbeitet, schalten Sie diese beiden Funktionen nicht aus. Weitere Informationen zum *Common Criteria Mode* erhalten Sie in Kapitel 5.1.12 auf Seite 129.

System Information



Packet Filter Live Log: Der **Packet Filter Live Log** dient zur Überwachung der gesetzten **Paketfilter**- und **NAT**-Regeln. Im Fenster werden in Echtzeit die Pakete angezeigt, die durch den Regelsatz des Paketfilters abgefangen werden. Diese Funktion eignet sich besonders zur Fehlersuche. Sollte nach der Inbetriebnahme des Internet-Sicherheitssystems eine Anwendung, z. B. Online-Banking, nicht verfügbar sein, können Sie anhand des *Packet Filter Live Log* nachvollziehen, ob und welche Pakete durch die Firewall abgefangen wurden.

Für die Ausgabefelder **Current Packet Filter Rules** und **Current NAT Rules** werden die aktuell gültigen Regeln direkt aus dem Betriebssystem-Kernel entnommen und dargestellt.



Durch einen Klick auf die Schaltfläche **Show** öffnen Sie ein Fenster, in dem die Regelverletzungen in der Reihenfolge ihres Auftretens in Echtzeit tabellarisch aufgelistet werden. Anhand der Hintergrundfarbe können Sie sehen, welche Aktion für die jeweilige Regelverletzung ausgeführt wurde:

- Rot: Das Paket wurde blockiert (Drop)
  Pakete, die aufgrund der Funktionen *Spoof Protection*, *Validate Packet Length* und *SYN Rate Limiter* blockiert wurden werden ebenfalls rot hinterlegt angezeigt.
- Gelb: Das Paket wurde zurückgewiesen (Reject)
- Grün: Das Paket wurde durchgelassen (Allow)

- Grau: Das Paket wurde durch eine Funktion aus dem Modul *Flood Protection* blockiert (Drop). Die Funktionen befinden sich im Menü **DoS / Flood Protection** und werden in Kapitel 5.4.4 ab Seite 234 beschrieben.

Live-Log-Filter setzen / zurücksetzen:

Mit Hilfe der Eingabefelder **IP Address / Netmask** und **Port** sowie dem Drop-down-Menü **Protocoll** können Sie das *Packet Filter Live Log* so einstellen, dass in der Tabelle nur Regelverletzungen mit bestimmten Attributen angezeigt werden. Der Filter wirkt sich auf die Regelverletzungen aus, die nach dem Einschalten der Funktion protokolliert werden. Der Filter wird durch einen Klick auf die Schaltfläche **Set** ausgeführt.

Durch einen Klick auf die Schaltfläche **Clear** wird der Filter wieder zurückgesetzt. Ab diesem Zeitpunkt werden wieder alle Regelverletzungen im *Packet Filter Live Log* angezeigt.

Durch einen Klick auf das Kontrollkästchen **Pause Log** können Sie die Aktualisierung anhalten und wieder fortsetzen.

Hinweis:

Beachten Sie, dass nur die abgearbeiteten Regeln protokolliert werden, bei denen im Regelsatz unter **Packet Filter / Rules** die Funktion **Log** aktiviert wurde!

Current System Packet Filter Rules: Im Fenster **Current System Packet Filter Rules** können fortgeschrittene Administratoren in Echtzeit das Ergebnis der Filterregeltabelle sehen und deren Umsetzung im Kernel. Des Weiteren werden auch alle systemgenerierten Filterregeln angezeigt.

Current System NAT Rules: Im Fenster **Current System NAT Rules** werden alle definierten und systemgenerierten NAT-Regeln aufgelistet.

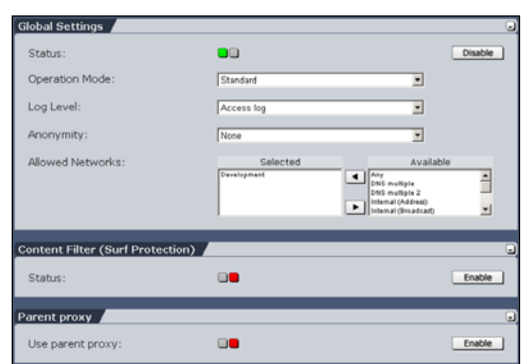
Connection Tracking Table: Im Fenster **Connection Tracking Table** wird der Netzwerkdatenverkehr analysiert und eine Liste mit den gegenwärtig erstellten Verbindungen dargestellt.

5.6. Application Gateways (Proxies)

Während der **Paketfilter (Packet Filter)** auf Netzwerk-Ebene den Datenverkehr filtert, wird durch den Einsatz von **Proxies (Application Gateways)** die Sicherheit der Firewall zusätzlich auf Application-Ebene erhöht, da zwischen Client und Server keine direkte Verbindung besteht.
Jeder **Proxy** kann speziell für seinen Dienst wiederum weitere Sicherheitsdienste anbieten. Durch das Wissen jedes Proxies um den Kontext seines Dienstes ergeben sich umfangreiche Sicherungs- und Protokollierungsmöglichkeiten. Die Analyse ist auf dieser Kommunikationsebene besonders intensiv möglich, da der Kontext der Anwendungsdaten jeweils klar durch Protokollstandards definiert ist. Die Proxies konzentrieren sich dabei auf das Wesentliche.

Im Verzeichnis **Proxies** wählen Sie die gleichnamigen **Proxies** aus und konfigurieren die Einstellungen. Zu Beginn sind alle **Proxies** ausgeschaltet. Die Firewall beinhaltet die Proxydienste **HTTP** (Web), **SMTP** (E-Mail), **POP3**, **DNS** (Nameserver), **Generic** (für die Nutzer von Novell eDirectory Directory), **SIP** (VoIP), **SOCKS** (Punkt-zu-Punkt-Verbindung), **Ident** und **Proxy Content Manager**.

5.6.1. HTTP



Im Menü **HTTP** konfigurieren Sie die Firewall als **HTTP-Cache-Proxy**. Dieser **Proxy** ist neben dem reinen Weiterleiten von WWW-Anfragen auch in der Lage, diese Seiten zwischenzuspeichern. Bereits zuvor angefragte Seiten werden dann nicht mehr über das Internet neu geladen, sondern nach der ersten Übertragung nur noch aus dem Cache des Proxies abgerufen.

Hinweis:

WebAdmin kann nicht über den eigenen Proxy aufgerufen werden. Die IP-Adresse des Sicherheitssystems muss daher im Browser von der Verwendung des Proxyservers ausgeschlossen werden.

Microsoft Explorer, Proxy für WebAdmin umgehen:

1. Öffnen Sie das Menü **Extras/Internetoptionen**.
2. Wählen Sie die Registerkarte **Verbindungen**.
3. Öffnen Sie das Menü **LAN-Einstellungen/Erweitert**.
4. Tragen Sie in das Eingabefeld unter **Ausnahmen** die IP-Adresse Ihrer Firewall ein.
5. Um die Eingaben zu speichern klicken Sie auf die Schaltfläche **OK**.

Mozilla Firefox, Proxy für WebAdmin umgehen:

1. Öffnen Sie das Menü **Extras/Einstellungen/Allgemein**.
2. Klicken Sie auf die Schaltfläche **Verbindungseinstellungen**.
3. Klicken Sie auf das Kontrollkästchen **Manuelle Proxy-Konfiguration**.

   Anschließend wird das Eingabemenü für die Konfiguration des Proxy aktiviert.
4. Tragen Sie in das Eingabefeld **Kein Proxy für** die IP-Adresse Ihrer Firewall ein.
5. Um die Eingaben zu speichern klicken Sie auf die Schaltfläche **OK**.

Netscape Communicator, Proxy für WebAdmin umgehen:

1. Öffnen Sie das Menü **Bearbeiten/Einstellungen/Erweitert/Proxies**.
2. Klicken Sie bei **Manuelle Proxies Konfiguration** auf die Schaltfläche **Anschauen**.
3. Tragen Sie in das Eingabefeld **Kein Proxy für** die IP-Adresse Ihrer Firewall ein.
4. Um die Eingaben zu speichern, klicken Sie auf die Schaltfläche **OK**.

Der **HTTP-Proxy** setzt das HTTP-Protokoll (im Allgemeinen TCP/IP-Port 80) zur Übertragung von Webseiten um. Hierbei sollte beachtet werden, dass Teile eines Webservers, z. B. Bilder aus einer Datenbank, nicht über Port 80 abgefragt werden, sondern über einen anderen TCP-Port. Falls Ihre Firewall im **Transparent**-Modus arbeitet, werden diese Anfragen nicht erfasst. Damit diese Anfragen von der

Firewall unterstützt werden, muss entweder ein anderer Modus eingestellt werden oder die Anfragen müssen durch eine entsprechende Regel im Menü **Packet Filter / Rules** behandelt werden.

Beispiel:

Source: ein lokales Netzwerk

Service: Dienst mit Zieladresse (Im Menü **Definitions / Services** müssen Sie zuvor diesen Dienst definieren)

Destination: IP-Adresse des Webservers oder **Any**

Action: Allow

HTTPS-Anfragen (TCP/IP-Port 443) werden unbearbeitet durch den Proxy weitergeleitet.

Hinweis:

Um den **Proxy** im Modus **Standard** verwenden zu können, muss der **Browser** entsprechend konfiguriert werden: **TCP / IP-Adresse der Firewall** und der im Menü **Proxies / HTTP** eingestellte **TCP Port**. Des Weiteren muss für den Proxydienst **HTTP** ein gültiger **Nameserver (DNS)** aktiviert sein. Ohne konfigurierten Browser kann der **Proxy** nur im Modus **Transparent** betrieben werden.

Global Settings

Die Betriebsmodi (Operation Modes)

Standard: Sie müssen alle Netzwerke auswählen, die in der Lage sein sollen, auf den HTTP-Proxy zuzugreifen. Alle nicht ausgewählten Netzwerke können nicht zugreifen, auch wenn der Proxy im Browser konfiguriert ist.
Wenn ein Zugriff auf das Word Wide Web ohne den HTTP-Proxy stattfinden soll, müssen Sie durch eine Regel im Menü **Packet Filter / Rules** den HTTP-Datenverkehr zwischen dem internen Netzwerk und dem Internet oder dem Webserver freigeben.

Beispiel:

Source: IP-Adresse des lokalen Client

Service: HTTP

Destination: IP-Adresse des Webservers oder **Any**

Action: Allow

Um über den Proxy auf das World Wide Web zuzugreifen, tragen Sie im Browser die IP-Adresse des Proxy – in der Regel die IP-Adresse der internen Netzwerkkarte - und die Portadresse 8080 ein.

Transparent: Die HTTP-Anfragen auf Port 80 aus dem internen Netzwerk werden abgefangen und durch den Proxy geleitet. Für den Browser des Endanwenders ist dieser Vorgang völlig unsichtbar. Es entsteht kein zusätzlicher Administrationsaufwand, da für den Browser des Endanwenders keine Einstellungen geändert werden müssen.
Alle Netzwerke, die transparent weitergeleitet werden sollen, müssen im Auswahlfeld **Allowed Networks** eingetragen sein. Im Modus **Transparent** ist es nicht möglich, durch etwaige Einstellungen im Browser Zugriff auf den HTTP-Proxy zu erhalten. Des Weiteren können in diesem Modus keine Daten von einem FTP-Server heruntergeladen werden. Ebenso müssen HTTPS-Verbindungen (SSL) über den Paketfilter (Packet Filter) abgewickelt werden.

User Authentication: Dieser Modus entspricht in der Funktionalität dem Modus **Standard**. Der Benutzer bekommt zusätzlich nur durch vorherige **Authentisierung** Zugriff auf den HTTP-Proxy.

Active Directory / NT Domain Membership: Dieser Modus steht zur Auswahl, wenn Sie im Menü die Authentifizierungsmethode **Active Directory / NT Domain Membership** konfiguriert haben.
Wenn dieser Betriebsmodus eingestellt ist, können nur die Benutzer auf den HTTP-Proxy zugreifen, die auf dem *Domain Controller* der Gruppe **http_access** zugehören.

Damit ein Benutzer Zugriff auf das Internet erhält, muss er in der **Profiles**-Tabelle einem bestimmten Profil zugeordnet sein. Wenn Sie

die Gruppe bereits im *Active Directory* (*AD*) definiert haben, müssen Sie dem Profil nur den selben Namen (hier: *http_access*) geben, wie der Gruppe im Verzeichnisdienst. Auf diese Weise müssen Sie nur die Profile für die Benutzergruppe definieren für die der Zugriff auf bestimmte Internetseiten verhindert werden soll.

Die Konfiguration der **Surf Protection Profiles** wird in Kapitel 5.6.1.1 ab Seite 279 beschrieben.

Hinweis:

Jede Änderung in **Proxies** wird ohne eine weitere Meldung sofort wirksam.

HTTP-Proxy einschalten:

1. Öffnen Sie im Verzeichnis **Proxies** das Menü **HTTP**.

2. Schalten Sie im Fenster **Global Settings** den Proxy durch einen Klick auf die Schaltfläche **Enable** ein.

   Anschließend öffnet sich ein erweitertes Eingabefenster.

3. Wählen Sie im Drop-down-Menü **Operation Mode** den Betriebsmodus aus.

   Beachten Sie bei den Betriebsmodi die jeweils notwendige Zusatzkonfiguration. Die Modi werden unter der Überschrift „Die Betriebsmodi (Operation Mode)" beschrieben.

   Wenn Sie den Betriebsmodus **Standard** oder **Transparent** eingestellt haben, fahren Sie mit Schritt 5 fort.

4. Falls Sie im Drop-down-Menü **Operation Mode** den Modus **User Authentication** ausgewählt haben, definieren Sie nun im Fenster **User Authentication** die Authentifizierungsmethode.

   Authentication Methods: Zur Auswahl stehen nur Authentifizierungsmethoden, die Sie zuvor im Menü **System/User Authentication** konfiguriert haben.

Falls Sie die Methode **Local Users** eingestellt haben, wählen Sie nun im Auswahlfeld **Allowed Users** die entsprechenden Benutzer aus. Die lokalen **Benutzer (Users)** werden im Menü **Definitions/Users** verwaltet.

5. Bestimmen Sie im Drop-down-Menü **Log Level** den von diesem Proxy generierten Informationsumfang.

   Full: Alle Daten werden protokolliert.

   Access Log: Nur die behandelten Daten werden protokolliert, z. B. die verwendeten URLs, die Benutzernamen und die IP-Adressen der Clients.

   None exept Content Filter: Es werden keine Daten für die Funktion **Caching** protokolliert. Die Einträge des Content Filter Log werden weiterhin geschrieben.

6. Bestimmen Sie im Drop-down-Menü **Anonymity** welche Informationen aus dem Netzwerk in den HTTP-Request-Headers versendet werden.

   Standard: Nur die hier aufgeführten Header-Typen werden blockiert: Accept-Encoding, From, Referrer, Server, WWW-Authenticate und Link.

   None: Die vom Client versendeten Header werden nicht geändert.

   Paranoid: Alle Header mit Ausnahme der nachfolgend aufgezählten Typen werden blockiert. Zusätzlich wird der Header "User-Agent" geändert, so dass keine Client-Versionsinformation das Netzwerk verläßt:
   Allow, Authorization, Cache-Control, Content-Encoding, Content-Length, Content-Type, Date, Expires, Host, If-Modified-Since, Last-Modified, Location, Pragma, Accept, Accept-Language, Content-Language, Mime-Version, Retry-After, Title, Connection, Proxy-Connection und User-Agent.

Hinweis:

Bei der Verwendung von **Standard** oder **Paranoid** werden Cookies vom Proxy blockiert. Falls Sie Cookies benötigen, sollten Sie die Einstellung **None** verwenden.

7. Wählen Sie im Auswahlfeld **Allowed Networks** die für diesen Proxy zugelassenen Netzwerke aus.

Wenn Sie in Schritt 3 den **Transparent Mode** eingestellt haben, wird hier zusätzlich das Auswahlfeld **Skip Source / Destination Networks** angezeigt. Hier haben Sie die Möglichkeit bestimmte Netzwerksegmente oder Hosts aus den erlaubten Netzwerken auszuklammern.

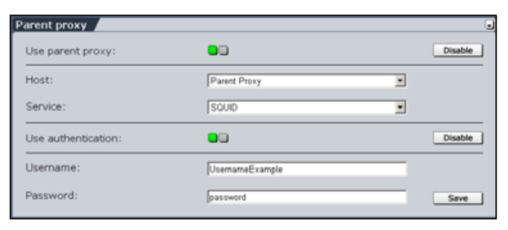
In den Auswahlmenüs können Netzwerke und Hosts ausgewählt werden, die zuvor im Menü **Definitions / Networks** definiert wurden.

Die Funktionsweise des **Auswahlfeldes** wird in Kapitel 4.3.2 ab Seite 41 beschrieben.

Alle Einstellungen werden sofort wirksam und bleiben beim Verlassen des Menüs erhalten. Aus den zugelassenen Netzwerken kann nun auf den HTTP-Proxy zugegriffen werden.

Beachten Sie auch die Funktionen im Fenster **Advanced**.

Parent Proxy



Die Funktion **Parent Proxy** wird in Ländern benötigt, in denen der Zugang zum Internet nur über einen staatlich kontrollierten Proxy erlaubt ist. Dies trifft auf viele Länder in Afrika oder Asien zu. Des Weiteren können in bestimmten IT-Landschaften hintereinanderliegende Proxys vorkommen. Sobald in diesem Fenster ein **Parent-Proxy** definiert wurde, werden die HTTP-Anfragen zuerst an die entsprechende IP-Adresse abgeschickt.

Parent-Proxy definieren:

1. Öffnen Sie im Verzeichnis **Proxies** das Menü **HTTP**.

2. Schalten Sie im Fenster **Parent Proxy** den Proxy durch einen Klick auf die Schaltfläche **Enable** ein.

   Anschließend öffnet sich ein erweitertes Eingabefenster.

3. Definieren Sie in den **Parent Proxy**.

   Host: Wählen Sie im Drop-down-Menü den Parent-Proxy-Server aus. Der Server muss zuvor im Menü **Definitions/Networks** definiert werden.

   Service: Wählen Sie im Drop-down-Menü den Dienst aus. Der Dienst muss zuvor im Menü **Definitions/Services** definiert werden.

4. Speichern Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

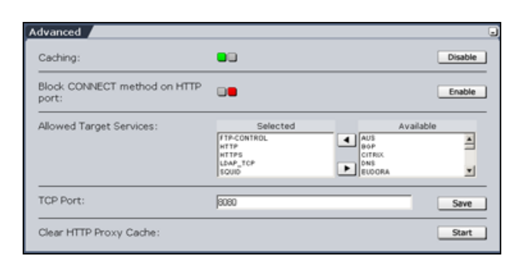
5. Falls für den **Parent Proxy** eine Authentifizierung notwendig ist, klicken Sie auf die Schaltfläche **Enable**.

Username: Tragen Sie in das Eingabefeld den Benutzernamen ein.

Password: Tragen Sie in das Eingabefeld das Passwort ein.

6. Speichern Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

Advanced



Caching: Mit dieser Funktion werden häufig verwendete Internetseiten im **HTTP Proxy Cache** zwischengespeichert. Per Default ist diese Funktion eingeschaltet (Statusampel zeigt Grün). Mit einem Klick auf die Schaltfläche **Disable** schalten Sie die Funktion aus.

Block CONNECT Method on HTTP Port: Jegliche HTTP-Verbindungsanfrage durch den HTTP-Proxy wird geblockt. Nur die HTTP-Methoden **GET** und **PUT** werden durch den Proxy geschickt. Dies hat auch zur Folge, dass keine HTTPS-Verbindungen aufgebaut werden können!

Jede Client Request wird durch die Angabe der Methode eingeleitet. Methoden bestimmen die Aktion der Anforderung. Die aktuelle HTTP-Spezifikation sieht acht Methoden vor: OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE und CONNECT. In diesem Abschitt werden nur die Methoden *GET* und *PUT* erklärt.
Die Methode **GET** dient zur Anforderung eines Dokuments oder einer anderen Quelle. Eine Quelle wird dabei durch den Request-URL identifiziert. Man unterscheidet zwei Typen: Conditional GET und partial GET. Beim Conditional-GET-Typ ist die Anforderung von Daten an Bedingungen geknüpft. Die genauen Bedingungen sind dabei im

Header-Feld Conditional hinterlegt. Oft gebrauchte Bedingungen sind z. B. If-Modified-Since, If-Unmodified-Since oder If-Match. Mit Hilfe dieser Bedingung lässt sich die Netzbelastung deutlich verringern, da nur noch die wirklich benötigten Daten übertragen werden. In der Praxis nutzen z. B. Proxyserver diese Funktion, um die mehrfache Übertragung von Daten, die sich bereits im Cache befinden, zu verhindern. Das gleiche Ziel verfolgt die partielle GET-Methode. Sie verwendet das Range-Header-Feld, das nur Teile der Daten überträgt, die der Client jedoch noch verarbeiten kann. Diese Technik wird für die Wiederaufnahme eines unterbrochenen Datentransfers verwendet.

Die Methode **PUT** erlaubt die Modifikation bestehender Quellen beziehungsweise Erzeugung neuer Daten auf dem Server. Im Unterschied zur POST-Methode identifiziert der URL in der PUT-Request die mit der Anforderung gesendeten Daten selbst, und nicht die Quelle.

Mit einem Klick auf die Schaltfläche **Enable** schalten Sie die Funktion ein (Statusampel zeigt Grün).

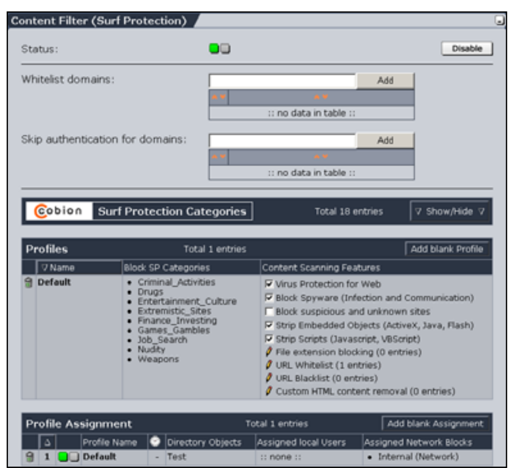
Allowed Target Services: Wählen Sie im Auswahlfeld die **Dienste** (**Services**) aus, auf die der HTTP-Proxy zugreifen kann. Per Default sind bereits die Dienste mit Ports enthalten, zu denen eine Verbindung als sicher gilt.

TCP Port: Tragen Sie in das Eingabefeld den **TCP/IP-Port** ein. Per Default ist hier bereits der TCP/IP-Port **8080** eingetragen.

Clear HTTP Proxy Cache: Häufig aufgerufene Seiten werden nicht mehr über das Internet neu geladen, sondern nach der ersten Übertragung nur noch aus dem **HTTP Proxy Cache** abgerufen.

Mit dieser Aktion wird der Inhalt des Caches durch einen Klick auf die Schaltfläche **Start** gelöscht.

5.6.1.1. Content Filter (Surf Protection)



Mit der Funktion **Surf Protection Profiles** werden Profile erstellt, um den Zugriff von einem Netzwerk oder nur von einzelnen Benutzern auf bestimmte Internetseiten, abhängig von der Kategorie der **URL**, zu verhindern. Die Kategorien basieren auf der **URL**-Datenbank von **Cobion Security Technologies** und können in der Tabelle **Surf Protection Categories** editiert werden.

Jedes *Surf Protection Profile* enthält einen **Content Filter** mit den Modulen **Virus Protection for Web** und **Spyware Protection** sowie weiteren *Schutzmechanismen*.

Das Modul **Spyware Protection** besteht aus den Funktionen:

- Block Spyware (Infection and Communication)
- Block suspicious and unknown sites

Die zusätzlichen *Schutzmechanismen* sind:

- Strip Embedded Objects
- Strip Scripts

Das Modul **Surf Protection** kann erst konfiguriert werden, wenn der HTTP-Proxy eingeschaltet ist. Die *Module* und *Schutzmechanismen* werden im Abschnitt **Die Profiles-Tabelle** beschrieben.
Die Informationen und Fehlermeldungen, die vom HTTP-Proxy zurückgesendet werden, sind in Kapitel 5.10.3.3 auf Seite 462 aufgeführt.

Hinweis:

Die Verbindung vom Content Filter zu Cobion erfolgt über den Port 6000. Wenn Sie z. B. eine Upstream Firewall einsetzen, kommt über diesen Port in der Regel keine Verbindung zustande. In diesem Fall baut das Sicherheitssystem automatisch die Verbindung zu Cobion mittels Port 80 (TCP) auf.

Whitelist Domains: In der Zugriffskontrollliste kann eine **Whitelist** mit Domänen definiert werden, die grundsätzlich vom **Surf Protection** ausgeschlossen werden.

Die Funktionsweise der **Zugriffskontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.5 ab Seite 43 beschrieben.

Skip Authentication for Domains: Mit der Zugriffskontrollliste kann eine **Whitelist** mit Domänen definiert werden, die von der NTLM-Authentisierung ausgeschlossen sein sollen. Dies ist für bestimmte Update-Mechanismen (z. B. Microsoft Windows Update) interessant, die keine NTLM-Authentisierung auf dem Proxy unterstützen.
Des Weiteren muss für die Domänen, die von der NTLM-Authentisierung ausgeschlossen sein sollen ein spezielles **Profil** (**Profile**) angelegt werden. Bei der **Profilzuweisung** (**Profile Assignment**) für dieses *Profil* müssen Sie in der Spalte **Assigned local Users** immer den Wert **none** einstellen. In der Spalte **Assigned Network Blocks** stellen Sie dann die Netzwerke ein, die auf diese speziellen Internetseiten zugreifen können sollen.

Die Definition und die Zuweisung von Profilen wird detailliert in den Abschnitten **Die Profile-Tabelle** und **Die Profile-Assignment-Tabelle** beschrieben.

Die Funktionsweise der **Zugriffskontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.5 ab Seite 43 beschrieben.

Surf Protection Categories

cobion Surf Protection Categories — Total 18 entries — Show/Hide

Name	Subcategories
Community_Education_Religion	• Cities/Countries/Regions • Government Institutions • Non Government Organizations • Partys • Religion • Sects • Upbringing/Education/Reconnoitring
Criminal_Activities	• Computer Criminalism • Hate and Discrimination • Illegal Activities • Warez Sites
Drugs	• Alcohol • Illegal Drugs • Self Help/Addiction • Tabacco
Entertainment_Culture	• Art/Museums • Belletristics/Specialized Books • Cinema, TV • Humor • Music • Theme Parks
Extremistic_Sites	• Extreme
Finance_Investing	• Accumulation of capital/Investing • Banking/Homebanking • Brokerage/Stock Exchange
Games_Gambles	• Computer Games • Gambles • Toys
Information_and_Communication	• Chat • Digital Postcards • General News, Newspaper and Magazines • Search Engines/Web Catalogs/Portals • SMS/Mobiles Fun • Usenet News and Bulletin Boards • Web Mail

Das Modul **Surf Protection** enthält 18 definierte **Surf Protection Categories**. Die Kategorien basieren auf der **URL**-Datenbank von **Cobion Security Technologies** und können in dieser Tabelle editiert werden.

Alle URLs, die in der *Cobion*-Datenbank enthalten sind, sind einer der 59 Unterkategorien (Subcategories) zugeordnet. Die Zuordnung erfolgt anhand von eindeutigen Kategorienamen, wie *Hate/Discrimination*, *Online Shopping* oder *Pornography*. Diese Inhaltskategorien können dazu genutzt werden um Internetseiten mit bestimmten Inhalten zu sperren. Fordert ein Benutzer eine Website an, so wird diese Anforderung mit der URL-Datenbank verglichen. Falls der Zugriff auf die Internetseite die vom Administrator definierte Web Policy verletzt, wird die Anfrage blockiert.

Die auf der URL-Datenbank kategorisierten Internetseiten sind nach den folgenden 18 Kategorien* bzw. 59 Unterkategorien unterteilt:

Community_Education_Religion*

(1) Governmental Organizations
Regierungsstellen und Behörden (z. B. Polizei, Feuerwehr und Krankenhäuser) sowie überstaatliche Regierungsstellen (z. B. Vereinte Nationen, Europäische Gemeinschaft.

(2) Non-Governmental Organizations
Nicht-staatliche Organisationen (z. B. Vereinigungen, Verbände, nicht gewinnorientierte Organisationen und Gewerkschaften).

(3) Cities/Regions/Countries
Regionale Informationen (z. B. Internetseiten von Städten, Regionen, Ländern, Stadtkarten).

(4) Education/Enlightenment
Bildungseinrichtungen (z. B. Universitäten, Hochschulen, öffentliche Schulen, Kindergärten, Erwachsenenbildung, Weiterbildung, Wörterbücher und Enzyklopädien jeder Art).

(5) Political Parties
Internetseiten über und von politischen Parteien.

(6) Religion
Internetseiten mit religiösem Inhalt (z. B. Informationen zu den fünf Hauptreligionen und religiöse Gemeinschaften, die aus diesen Religionen entstanden).

(7) Sects
Internetseiten zu Sekten (z. B. Kulte, Psycho-Gruppen, okkulte Gruppen).

Criminal_Activities*

(8) Illegal Activities
Beschreibungen zu illegalen Aktivitäten entsprechend der deutschen Rechtsprechung (z. B. Anleitungen zu Mord oder zum Bau von Bomben, Kinderpornografie).

(9) Computer Crime
Anleitungen zu illegalen Manipulationen an elektronischen Geräten (z. B. Methoden der Passwortverschlüsselung und -entschlüsselung, Virenprogrammierung, Kreditkartenmissbrauch)

(10) Hate and Discrimination
Internetseiten mit Hasstiraden und diskriminierenden Inhalten (z. B. rechts- und linksextreme Gruppen, sexistische und rassistische

Ansichten und Internetseiten, die die Unterdrückung von Minoritäten propagieren.

(11) Hacking
Informationen zu Hacks und Cracks (z. B. Lizenzschlüssel-Listen und illegale Lizenzschlüssel-Generatoren).

Drugs*

(12) Illegal Drugs
Informationen zu illegalen Drogen (z. B. LSD, Heroine, Kokain, XTC, Haschisch, Amphetamine sowie Hilfsmittel zum Drogengebrauch).

(13) Alcohol
Internetseiten mit verharmlosenden Inhalten zum Alkoholkonsum (z. B. Wein, Bier, Likör und Brauereien) sowie die Internetseiten von Händlern alkoholischer Getränke.

(14) Tobacco
Internetseiten über Tabak und Rauchen (z. B. Zigarren, Zigaretten, Pfeifen) sowie die Internetseiten von Tabakwarenhändlern.

(15) Self Help/Addiction
Internetseiten von Selbsthilfegruppen, Eheberatungen und Suchtberatungsstellen.

Entertainment_Culture*

(16) Cinema/Television
Kinos und sonstige Film- und Fernsehangebote (z. B. Programminformationen und Video on Demand).

(17) Amusement/Theme Parks
Freizeitveranstalter (z. B. öffentliche Schwimmbäder, Zoos, Messen und Vergnügungsparks).

(18) Art/Museums
Internetseiten zu kulturellen Veranstaltungen und Museen (z. B. Theater, Museen, Ausstellungen und deren Öffnungszeiten).

(19) Music

Internetseiten zu Musikanbietern (z. B. Radiostationen, MP3, Real Audio, Microsoft Media, Internetseiten zu Music Bands, Plattenfirmen und Musikanbietern).

(20) Literature/Books

Literatur und Bücher (z. B. Romane, Fachbücher, Kochbücher, Ratgeber usw.).

(21) Humor/Comics

Internetseiten mit humoristischen Inhalten (z. B. Witze, Sketche).

Extremistic Sites*

(22) Extremistics

Internetseiten mit extremen Inhalten (z. B. extrem gewalttätig). Diese URLs sind in der Regel auch in anderen Unterkategorien enthalten.

Finance_Investing*

(23) Brokerage

Internetseiten mit Börsenticker, die ausschließlich Vermittlungsgeschäfte betreiben (z. B. Finanzierung, Maklergeschäfte, Online-Wertpapierhandel).

(24) Investing

Internetseiten zu Immobilien (z. B. Baufinanzierung, Versicherungen).

(25) Banking

Internetseiten von Banken und zur Kontoführung (z. B. Zweigstellen, Genossenschaftsbanken und Online-Bankkonten).

Games_Gambles*

(26) Gambling

Internetseiten von Glücksspieleinrichtungen (z. B. Kasinos, Wettbüros und Lotterien).

(27) Computer Games

Informationen zu Computerspielen (z. B. Computerspielproduzenten, Internetseiten mit Cheat-Codes und Online-Spielzonen).

(28) Toys

Informationen zu Spielwaren (z. B. Puppen, Modellbau, Brettspiele, Karten- und Gesellschaftsspiele, Modellieren).

Information_Communication*

(29) General News/Newspapers/Magazines

Informationen zum allgemeinen Geschehen (z. B. Zeitungen und Zeitschriften).

(30) Web Mail

Internetseiten, über die E-Mails gesendet und empfangen werden können. In dieser Unterkategorie sind alle Web Mail Provider kategorisiert.

(31) Chat

Internetseiten, über die ein direkter Nachrichtenaustausch mit anderen Benutzern durchgeführt wird. In dieser Unterkategorie sind auch alle Chat Provider kategorisiert.

(32) Newsgroups/Bulletin New Boards/Discussion Sites

Internetseiten mit Informationen zu unterschiedlichen Themen, die wie an einem Schwarzen Brett angeboten werden.

(33) SMS/Mobile Phones fun Applications

Internetseiten mit Funktionen, um kurze Nachrichten mittels SMS an Mobiltelefone zu schicken. Hier sind auch die Anbieter von Zusatzgeräten für Mobiltelefone kategorisiert (z. B. Klingeltöne, Spiele, Cover).

(34) Digital Postcards

Internetseiten mit Funktionen, um digitale Postkarten zu senden.

(35) Search Engines/Web Catalogs/Portals

Internetseiten mit Suchmaschinen, Netkataloge und Netzportale.

IT*

(36) Software and Hardware Vendors/Distributors
Internetseiten von Hardware-Produzenten für Informations-, Mess- und Modultechnologie, Verkäufer von Software und Händler von Hard- und Software, Web-Hosting, Internet Service Provider sowie Anbieter von Breitbanddiensten.

(37) Web Hosting
Internetseiten über Web Hosting und von Internet Service Provider sowie von Provider von Breitbanddiensten.

(38) Information Security Sites
Informationen über Sicherheit, Privatsphäre und Datenschutz im Internet sowie in anderen Telekommunikations-Breitbanddiensten.

(39) URL Translation Sites
Internetseiten mit Funktionen zur Übersetzung von Teilen oder des gesamten Inhalts einer Internetseite in eine andere Sprache.

(40) Anonymous Proxies
Internetseiten über die Benutzer anonym im World Wide Web surfen können.

Job_Search*

(41) Job Search
Internetseiten zur Stellensuche (z. B. Arbeitsangebote, Arbeitssuchende, Arbeitsvermittler, Arbeitsämter, Zeitarbeit, etc.).

Lifestyle*

(42) Dating/Relationship
Internetseiten zur Förderung von zwischenmenschlichen Beziehungen.

(43) Restaurant/Bars
Internetseiten über Gaststätten (z. B. Restaurants, Bars, Diskotheken, Schnellimbissgaststätten).

(44) Travel
Internetseiten zum Thema Reisen (z. B. Denkmäler, Gebäude, Sehenswürdigkeiten, Reisebüros, Hotels, Animationsprogramme, Motels, Fluglinien, Eisenbahnen, Autovermietungen und Touristikinformation).

(45) Fashion/Cosmetics/Jewelry
Internetseiten über Mode, Kosmetik, Schmuck, Parfüms, Informationen zum Modeln und Model-Agenturen.

(46) Sports
Internetseiten über Fanclubs, Events (z. B. Olympische Spiele, Weltmeisterschaften), Sportresultate, Vereine, Mannschaften und Sport-Vereinigungen.

(47) Building/Residence/Furniture
Internetseiten über Gebäude- und Innenausstattungen (z. B. Immobilienmärkte, Möbelmärkte, vorfabrizierte Häuser, Design, etc.).

(48) Nature/Environment
Internetseiten über Natur und Umwelt (z. B. Umweltschutz, Haustiere, Gartenmärkte, etc.).

Locomotion*

(49) Locomotion
Internetseiten zu Fortbewegungsmitteln jeglicher Art (z. B. Freizeitfahrzeuge, Tuning, Autoausstellungen, Motorräder, Flugzeugen, Schiffen, Unterseebooten, Fahrrädern, Eisenbahnen, etc.).

Medicine*

(50) health/Recreation/Nutrition
Internetseiten zu Gesundheit, Erholung und Ernährung (z. B. Krankenhäuser, Doktoren, Drug Stores, Reformhäuser, Psychologie, Krankenpflege, Medizin, etc.).

(51) Abortion
Internetseiten mit Informationen zu Schwangerschaftabbrüchen.

Nudity*

(52) Pornography

Internetseiten mit eindeutigen sexuellen Handlungen und erotischen Inhalten, die für Kinder und Jugendliche unter 18 Jahren nicht geeignet sind.

(53) Erotic/Sex

Internetseiten mit erotischen Fotografien und sonstigem erotischen Material, das in dieser und ähnlicher Form auch über das Fernsehen oder über Zeitschriften zugänglich ist. In dieser Kategorie sind auch Sex Toys enthalten. Internetseiten mit eindeutige sexuelle Handlungen sind hier nicht enthalten.

(54) Swimwear/Lingerie

Internetseiten mit Bade- und Unterwäschemode, bzw. Nacktheit in ähnlicher Form (z. B. Bikini- und Strandmode, Damenunterwäsche, etc.).

Ordering*

(55) Online Purchasing

Internetseiten mit Warenangeboten, die oline bestellt werden können.

(56) Auctions/Small Advertisements

Internetseiten von Online- und Offline-Auktionshäusern, Versteigerungen und Online- und Offline-Werbung.

Private_Homepages*

(57) Private Homepages

Private Webauftritte und Internetseiten von Homepage-Servern.

Suspicious_and_Uncategorized*

(58) Suspicious and Uncategorized

Weapons*

(59) Weapons

Internetseiten auf denen mit Waffen und Zubehör verschiedener

Art (z. B. Luftgewehre, Explosionsstoffe, Munition, militärische Waffen, Jagdwaffen, Schwerter) oder auch mit Messern (ausschließlich Haushalts- oder Taschenmesser) gehandelt wird.

Die Hauptkategorien können auch durch Unterkategorien aus einer der anderen Kategorien ergänzt werden. Das Editieren der *Surf Protection Categories* wird im nachfolgenden Abschnitt beschrieben.

Surf Protection Categories editieren:

1. Schalten Sie das Modul im Fenster **Content Filter (Surf Protection)** durch einen Klick auf die Schaltfläche **Enable** ein.

Die Statusampel zeigt Grün und ein erweitertes Eingabefenster wird geöffnet.

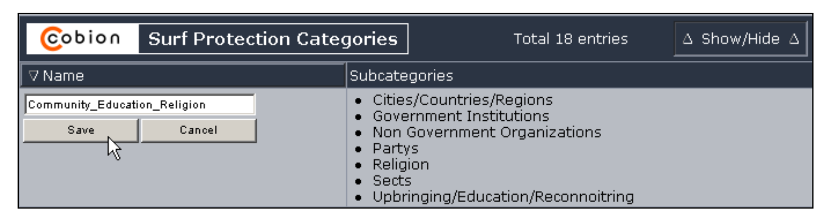
2. Öffnen Sie durch einen Klick auf die Schaltfläche **Show / Hide** die Tabelle mit den Kategorien.

Im Feld **Name** wird der Name der Kategorie angezeigt. Dieser Name wird später in der *Profile-Tabelle* ausgewählt. Im Feld **Subcategories** werden die Unterkategorien auggelistet.

3. Klicken Sie nun auf den Eintrag den Sie editieren möchten.

Beim Klick auf den **Namen** (**Name**) öffnet sich ein Eingabefenster. Hier können Sie den Namen der Kategorie editieren.

Wenn Sie auf die **Unterkategorien** (**Subcategories**) klicken wird ein Auswahlfeld geöffnet. In diesem Auswahlfeld befinden sich alle verfügbaren Unterkategorien. Hier können Sie der *Kategorie* weitere *Unterkategorien* hinzufügen.



Mit der Schaltfläche **Save** wird die Änderung gespeichert. Durch einen Klick auf die Schaltfläche **Cancel** wird der alte Eintrag beibehalten.

4. Schließen Sie die Tabelle durch einen Klick auf die Schaltfläche **Show / Hide**.

Anschließend wird das Fenster **Surf Protection Categories** geschlossen.

Die Profiles-Tabelle

Jedes **Surf Protection Profile** wird in der Tabelle **Profiles** duch eine separate Zeile dargestellt: Die Einstellungen können durch einen Klick auf das entsprechende Feld editiert werden.

Ein **Surf Protection Profile** enthält zwei Funktionsgruppen: Die **Surf Protection Categories**, mit den Zusatzfunktionen *URL Blacklist, URL Whitelist* und *Custom HTML Content Removal*, und den **Content Filter**. Mit Hilfe der *Surf Protection Categories* wird der Zugriff auf Internetseiten mit einem bestimmten Informationsinhalt verhindert. Der *Content Filter* enthält die Module *Virus-Protection for Web* und *Spyware Protection* und filtert zudem Internetseiten mit bestimmten technischen Komponenten.
Die Informationen und Fehlermeldungen, die vom HTTP-Proxy zurückgesendet werden, sind in Kapitel 5.10.3.3 auf Seite 462 aufgeführt.

Die Funktionen

Das nachfolgende Bild zeigt ein **Surf Protection Profile**:

Profiles — Total 1 entries — Add blank Profile

	∇ Name	Block SP Categories	Content Scanning Features
	Default	• Information_and_Communication	☑ Virus Protection for Web ☑ Block Spyware (Infection and Communication) ☐ Block suspicious and unknown sites ☑ Strip Embedded Objects (ActiveX, Java, Flash) ☑ Strip Scripts (Javascript, VBScript) File extension blocking (0 entries) URL Whitelist (1 entries) URL Blacklist (0 entries) Custom HTML content removal (0 entries)

Die Funktionen von links nach rechts sind:

Profile löschen ( ): Durch einen Klick auf das Papierkorb-Symbol wird das Profil aus der Tabelle gelöscht.

Name: Dies ist der Name des Surf Protection Profile. Der *Name* wird benötigt, um das Profil einem bestimmten *Netzwerk (Network)* oder einem *Benutzer (User)* zuzuweisen.
Das Editierfenster wird durch einen Klick auf das Feld mit dem Eintrag (z. B. Default) geöffnet. Mit der Schaltfläche **Save** wird die Änderung gespeichert. Durch einen Klick auf die Schaltfläche **Cancel** wird der alte Eintrag beibehalten.

Block SP Categories: In diesem Feld wählen Sie die Themen der Internetseiten aus, die für dieses Profil gesperrt sein sollen. Das Auswahlfenster wird durch einen Klick auf den Eintrag (z. B. 0 entries) geöffnet.

Das Modul **Surf Protection** enthält 18 definierte **Surf Protection Categories**. Diese 18 Kategorien werden in der gleichnamigen Tabelle verwaltet und editiert.

Die Verwaltung der **Surf Protection Categories** wird ab Seite 289 beschrieben.

Virus Protection for Web: Mit dieser Funktion werden die eingehenden Daten auf potentiell gefährliche Inhalte, wie z. B. Viren

untersucht. Durch einen Klick auf das Kontrollkästchen wird **Virus Protection for Web** ein- und ausgeschaltet.

Block Spyware (Infection and Communication): Diese Funktion entdeckt und blockiert *Spyware*, die vom Server zum Client geladen wird. Dadurch wird verhindert, dass der Computer mit neuer *Spyware* infiziert wird. Zusätzlich kann diese Funktion den Datenverkehr zwischen der bereits auf einem Client installierten *Spyware* und dem Internet erkennen und unterbinden. Die *Spyware* ist somit nicht mehr in der Lage die von ihr gesammelten Informationen an den Empfänger weiterzuleiten.

Bei *Spyware* handelt es sich um Anwendungen, die Informationen über einen Benutzer und seine Surfgewohnheiten sammeln und diese über das Internet versenden, ohne dass der Benutzer darüber informiert, geschweige den sein Einverständnis eingeholt wird.
Der Begriff *Spyware* umfasst ebenfalls so genannte *Adware*, *Malware* oder andere Anwendungen dieser Art, die das System eines Benutzers ausspionieren oder gefährden. *Spyware* ist aus mehreren Gründen gefährlich:
Sicherheitslücke für Informationen und Daten - im schlimmsten Fall enthält sie ein Tool, mit dem jede Eingabe erfasst und aufgezeichnet wird, u.a. auch die Eingabe von Passwörtern. Hinter der Entwicklung stehen oft gewerbliche Händler, da *Spyware* meist zur Erfassung des Kundenverhaltens verwendet werden:

- Die *Spyware* wird in der Regel unbemerkt installiert und ausgeführt
- Die *Spyware* lässt sich nur schwer identifizieren und entfernen
- Die Kommunikation der *Spyware* mit dem Internet kann von den meisten Desktop Firewalls nicht von zulässigem Datenverkehr unterschieden werden

Eine typische *Spyware* installiert sich so, dass sie jedes Mal automatisch startet, wenn der Computer hochgefahren wird. Sie ist permanent aktiv. Die *Spyware* registriert das Surfverhalten des An-

wenders und gibt diese Daten an externe Systeme weiter, die damit gezielte Werbung an diesen Anwender versenden. In der Regel beschädigt *Spyware* die Dateien des Benutzers nicht. Der größte Schaden, den *Spyware* anrichtet, entsteht durch die Erfassung und Verwendung der personenbezogenen Daten. *Spyware* installiert sich zumeist durch eine der folgenden Methoden:

- Eine versteckte *Spyware*-Komponente ist in einem anderen, gewünschten Programm integriert. So kann zum Beispiel die Zulassung zu web-basierten Anwendungen oftmals mit *Spyware* verknüpft sein, z. B. mit bestimmten Werkzeugleisten.
- Unbemerkte Direktinstallation auf einen Computer über einen so genannten *Drive-by* Download ohne Aufforderung des Benutzers. Zu diesen *Drive-by* Installationen gehören auch oftmals die so genannten *Browser Helper Objects,* die sich selbst als Teil eines Webbrowsers einbetten und das Surfverhalten des Benutzers aufzeichnen.
- HTTP Cookies zum Aufzeichnen des Verhaltens des Benutzers. Bei einem Cookie handelt es sich um einen Mechanismus zum Speichern der vom Benutzer besuchten Internetseiten auf dessen eigenem Computer. Diese werden oftmals dazu verwendet, die individuellen Surfgewohnheiten nicht nur für bestimmte Internetseiten aufzuzeichnen, sondern für alle Webseiten, die ein Benutzer in einem bestimmten Zeitraum aufgerufen hat. Dies ist jedoch erst dann gefährlich, wenn dahinter ein Unternehmen steht, das so das Surfverhalten über mehrere Seiten nachverfolgt.

Bei der Funktion **Block Spyware** handelt es sich um die *Cobion*-Unterkategorie *Spyware (60)*. Wenn diese Funktion eingeschaltet ist, werden die angeforderten Internetseiten mit den URLs dieser *Unterkategorie* (*Sub-category*) verglichen. Wenn die angeforderte Internetseite darin kategorisiert ist, wird sie geblockt. Die Unterkategorie *Spyware* ist keiner der 18 Hauptkategorien zugeordnet. Sie sollte nur durch das Kontrollkästchen **Block Spyware** aktiviert werden.

Block suspicious and unkown sites: Mit dieser Funktion wird verhindert, dass der Browser Internetseiten mit unbekanntem Inhalt öffnet. Diese Funktion kann als zusätzliche Sicherung angesehen werden, falls eine durch *Spyware* kontaminierte Internetseite noch nicht als solche kategorisiert wurde.

Diese Funktion bewahrt den Benutzer außerdem vor sogenannten *Phishing*-Angriffen, da die *Phishing Mails* in der Regel verdächtige Links enthalten. Diese Links werden geblockt, wenn Sie bereits als *Uncategorized (Cobion-Sub-category 73)*, *Categorization Failed (74)*, oder *Suspicious (75)* kategorisiert sind. Falls die *Phishing Mail* trotzdem angekommen ist, wird dadurch auch verhindert, dass der Benutzer auf den Link klickt.
Neben den potentiell kontaminierten URLs kann es auch vorkommen, dass reguläre Internetseiten für Online Banking, die von den *Phishers* häufig gefälscht werden, kategorisiert werden. Dies kann auch andere URLs betreffen, die eigentlich erlaubt sein sollten. Um den Zugang auf diese Internetseiten zu gewähren, können diese in die Zugriffskontrollliste *URL Whitelist* eingetragen werden.

Strip Embedded Objects: Mit dieser Funktion werden in angeforderten Internetseiten die eingebetteten Objekte, wie ActiveX, Flash oder Java entfernt.



Sicherheitshinweis:

Schalten Sie die Funktion **Strip Embedded Objects** nur ein, wenn für Ihr Netzwerk hohe Sicherheitsanforderungen bestehen.

Durch einen Klick auf das Kontrollkästchen wird **Strip Embedded Objects** ein- und ausgeschaltet.

Strip Scripts: Mit dieser Funktion werden aus dem eingehenden HTTP-Datenverkehr Script-Inhalte, wie Java- und VBScript entfernt.



Sicherheitshinweis:

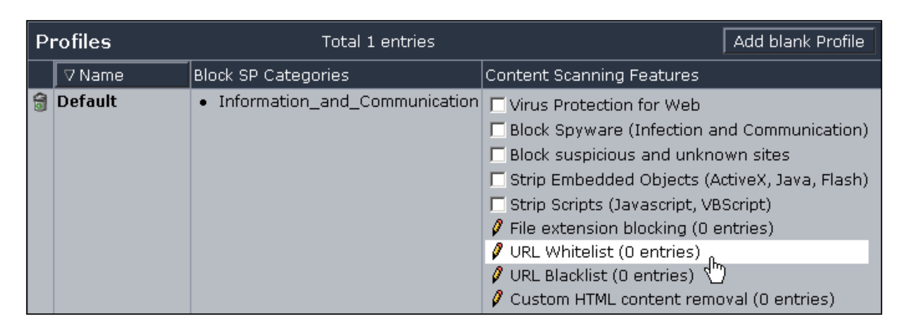
Schalten Sie die Funktion **Strip Scripts** nur ein, wenn für Ihr Netzwerk hohe Sicherheitsanforderungen bestehen.

Durch einen Klick auf das Kontrollkästchen wird der **Strip Scripts** ein- und ausgeschaltet.

File extension blocking: Mit dieser Funktion werden Dateien mit den Erweiterungen aus der Kontrollliste blockiert.

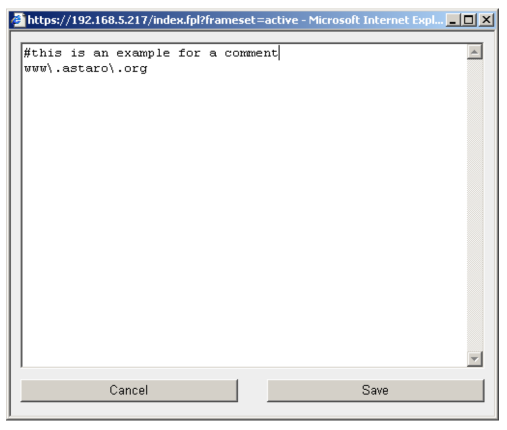
Die Zugriffskontrollliste wird durch einen Klick auf die Zeile mit dem Eintrag (z. B. 0 entries) geöffnet. Tragen Sie die Erweiterungen untereinander in das Eingabefeld ein. Achten Sie hierbei darauf, dass nur der String „exe“ in der Zeile steht, und nicht noch zusätzlich der Punkt vor der Erweiterung (richtig: exe, falsch: .exe). Kommentare müssen durch das Zeichen **#** am Anfang jeder Zeile gekennzeichnet werden. Mit der Schaltfläche **Save** werden die Änderungen gespeichert. Durch einen Klick auf die Schaltfläche **Cancel** wird der alte Eintrag beibehalten.

URL Whitelist: Dies ist eine Zusatzfunktion von **Block SP Categories**. Mit dieser Zugriffskontrollliste können Sie den Zugriff auf bestimmte Internetseiten „erlauben“, deren Inhalt eigentlich den *Surf-Protection-Categories*-Themen entsprechen.



Beispiel: Sie haben in der Spalte **Surf Protection Categories** das Thema **Information and Communication** ausgewählt, möchten aber den Zugriff auf die Internetseite **www.astaro.org** erlauben,

dann legen Sie zusätzlich eine **URL Whitelist** an, indem Sie die Internetadresse in die Zugriffskontrollliste eintragen.



Die Zugriffskontrollliste wird durch einen Klick auf die Zeile mit dem Eintrag (z. B. 0 entries) geöffnet. Tragen Sie die Internetadressen untereinander in das Eingabefeld ein (z. B. www\.astaro\.org). Kommentare müssen durch das Zeichen **#** am Anfang jeder Zeile gekennzeichnet werden. Mit der Schaltfläche **Save** werden die Änderungen gespeichert. Durch einen Klick auf die Schaltfläche **Cancel** wird der alte Eintrag beibehalten.

URL Blacklist: Dies ist eine Zusatzfunktion von **Block SP Categories**. Mit dieser Zugriffskontrollliste können Sie zusätzlich bestimmte Internetseiten, deren Inhalt eigentlich keinem der *Surf-Protection-Categories*-Themen entsprechen, für den Zugriff ausschließen.

Die Zugriffskontrollliste wird durch einen Klick auf die Zeile mit dem Eintrag (z. B. 0 entries) geöffnet. Tragen Sie die Internetadressen untereinander in das Eingabefeld ein. Kommentare müssen durch das Zeichen **#** am Anfang jeder Zeile gekennzeichnet werden.
Mit der Schaltfläche **Save** werden die Änderungen gespeichert. Durch einen Klick auf die Schaltfläche **Cancel** wird der alte Eintrag beibehalten.

Custom HTML Content Removal: Dies ist eine Zusatzfunktion von **Block SP Categories**. Mit dieser Zugriffskontrollliste können Sie in Echtzeit Internetseiten filtern (Online Filtering), die bestimmte Begriffe enthalten. Texte, die einen Begriff aus der Zugriffskontrollliste enthalten, werden durch einen HTML-Kommentar ersetzt.

Die Zugriffskontrollliste wird durch einen Klick auf das Verzeichnis mit dem Eintrag (z. B. 0 entries) geöffnet. Tragen Sie die Ausdrücke untereinander in das Eingabefeld ein. Kommentare müssen durch das Zeichen **#** am Anfang jeder Zeile gekennzeichnet werden.
Mit der Schaltfläche **Save** werden die Änderungen gespeichert. Durch einen Klick auf die Schaltfläche **Cancel** wird der alte Eintrag beibehalten.

Surf Protection einschalten, Profile hinzufügen:

1. Schalten Sie das Modul im Fenster **Surf Protection (Content Filter)** durch einen Klick auf die Schaltfläche **Enable** ein.

   Die Statusampel zeigt Grün und ein erweitertes Eingabefenster wird geöffnet.

   Per Default enthält die Tabelle **Profiles** ein **Blanko-Surf-Protection-Profile**.

2. Um ein neues **Blanko-Surf-Protection-Profile** in die Tabelle einzufügen klicken Sie auf die Schaltfläche **Add blank Profile**.

Anschließend können Sie das *Surf Protection Profile* editieren.

Surf Protection Profile editieren:

1. Gehen Sie in der Tabelle **Profiles** zu dem *Surf Protection Profile*, das Sie editieren möchten.

2. Tragen Sie in das Feld **Name** einen eindeutigen Namen für das *Surf Protection Profile* ein.

3. Führen Sie die Einstellungen für die Funktionsgruppe **Surf Protection Categories** in der nachfolgend aufgeführten Reihenfolge durch.

   Block SP Categories: Wählen Sie in diesem Feld die Themen der Internetseiten aus, die von Ihrem Netzwerk aus nicht geöffnet werden sollen.

URL Whitelist: Tragen Sie in die Zugriffskontrollliste die Internetadressen ein, auf die der Zugriff „erlaubt" ist, obwohl sie einem Thema im Feld **Surf Protection Categories** entspricht.

URL Blacklist: Tragen Sie in die Zugriffskontrollliste die Internetadressen ein, auf die der Zugriff „nicht erlaubt" ist, obwohl sie keinem der Themen im Feld **Surf Protection Categories** entsprechen.



Sicherheitshinweis:

Beim HTTP-Protokoll wird der Header vom **HTTP-Cache-Proxy Squid** gefiltert.

Anderst beim **HTTPS**-Protokoll - hier wird der Header nur durchlaufen. Das Modul **Surf Protection** kann daher bei **HTTPS**-Verbindungen keine angefragte **URL** aufgrund der **White-** oder **Blacklist** bewerten.

Custom HTML Content Removal: Tragen Sie in die Zugriffskontrollliste die Begriffe ein, die aus den Internetseiten entfernt werden sollen.

4. Führen Sie die Einstellungen für die Funktionsgruppe **Content Scanning Features** durch.

   Virus Protection for Web: Durch einen Klick auf das Kontrollkästchen wird die Funktion ein- und ausgegeschaltet.

   Block Spyware (Infection and Communication): Durch einen Klick auf das Kontrollkästchen wird die Funktion ein- und ausgegeschaltet.

   Block suspicious and unkown sites: Durch einen Klick auf das Kontrollkästchen wird die Funktion ein- und ausgegeschaltet.

   Strip Embedded Objects: Durch einen Klick auf das Kontrollkästchen wird der Filter ein- und ausgegeschaltet.



Sicherheitshinweis:

Schalten Sie die Funktion **Strip Embedded Objects** nur ein, wenn für Ihr Netzwerk hohe Sicherheitsanforderungen bestehen.

Strip Script: Durch einen Klick auf das Kontrollkästchen wird die Funktion ein- und ausgegeschaltet.



Sicherheitshinweis:

Schalten Sie die Funktion **Strip Script** nur ein, wenn für Ihr Netzwerk hohe Sicherheitsanforderungen bestehen.

File extension blocking: Mit dieser Funktion werden Dateien mit den Erweiterungen aus der Kontrollliste blockiert.

Das **Surf Protection Profile** ist nun ediert. Weisen Sie nun das *Profile* in der Tabelle **Profile Assignment** einem *Netzwerk (Network)* oder einem *lokalen Benutzer (Local User)* zu.

Die Profile-Assignment-Tabelle

In der Tabelle **Profile Assignment** werden die **Surf Protection Profiles** aus der Tabelle **Profiles** den lokalen Benutzern (Local Users) oder Netzwerken (Networks) zugewiesen.

Damit ein *Surf Protection Profile* einem lokalen Benutzer zugewiesen werden kann, muss der HTTP-Proxy im **User-Authentication**-Modus betrieben werden. Einem Netzwerk hingegen kann in jedem Betriebsmodus ein *Profile* zugewiesen werden.

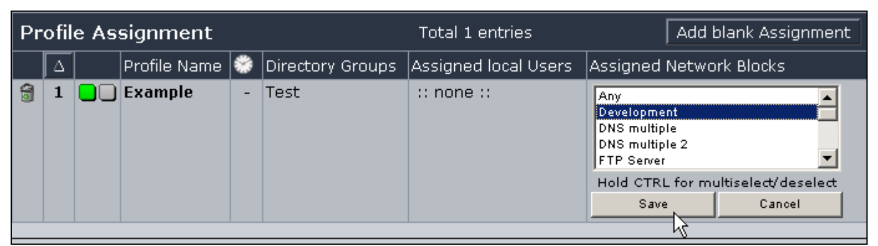
Wichtiger Hinweis:

Wenn Sie einem **Profile** gleichzeitig einen **lokalen Benutzer** und ein **Netzwerk** zuweisen, dann wird das *Profile* nur wirksam, wenn der Benutzer auch aus dem „eingestellten" Netzwerk auf den HTTP-Proxy zugreift! Einem lokalen Benutzer oder einem Netzwerk kann immer nur ein **Surf Protection Profile** zugeordnet werden.

Wenn Sie im Fenster **Global Settings** den Betriebsmodus **User Authentication** eingestellt haben, wird über der Tabelle *Profile Assignment* das Drop-down-Menü **Profile Assignment via** angezeigt. Per Default ist **Local Users + Network blocks** eingestellt.

Die Funktionen

Das nachfolgende Bild zeigt eine **Profile-Zuweisung**:



Die Funktionen von links nach rechts sind:

Profile-Zuweisung löschen (): Durch einen Klick auf das Papierkorb-Symbol wird die Zuweisung aus der Tabelle gelöscht.

Positionsnummer: Die Reihenfolge der Abarbeitung wird in der Tabelle durch die **Positionsnummer** angezeigt.
Durch einen Klick auf das Feld mit dem Eintrag wird ein Drop-down-Menü geöffnet. Über dieses Drop-down-Menü können Sie nun die Reihenfolge der Profile-Zuweisungen ändern. Mit der Schaltfläche **Save** werden die Änderungen gespeichert. Durch einen Klick auf die Schaltfläche **Cancel** wird der alte Eintrag beibehalten.

Statusampel: Durch die Ampel wird der Status der Profile-Zuweisung angezeigt: Jede neue Zuweisung ist ausgeschaltet (Statusampel zeigt Rot).
Die Profile-Zuweisung wird durch einen Klick auf die Statusampel eingeschaltet (Statusampel zeigt Grün).

Profile Name: In diesem Feld wählen Sie das **Surf Protection Profile** aus der Profile-Tabelle aus.
Durch einen Klick auf das Feld mit dem Eintrag wird das Drop-down-Menü geöffnet. Mit der Schaltfläche **Save** werden die Änderungen gespeichert. Durch einen Klick auf die Schaltfläche **Cancel** wird der alte Eintrag beibehalten.

Time Event (): Durch einen Klick auf das Feld in dieser Spalte wird ein Dop-down-Menü geöffnet. Nun können Sie das Zeitintervall für das Profil auswählen. Durch einen Klick auf die Schaltfläche **Save** werden die Änderungen gespeichert. Um den Vorgang abzubrechen klicken Sie auf die Schaltfläche **Cancel**.
Wenn für ein Profil ein Zeitintervall eingestellt ist, wird im entsprechenden Feld das Uhren-Symbol angezeigt. Die genauen Einstellungen für dieses Zeitintervall werden angezeigt, wenn Sie mit der Maus dieses Uhrensymbol berühren.

Die Zeitinterwalle werden im Menü **Definitions/Time Events** definiert. Das Menü wird in Kapitel 5.2.4 ab Seite 150 beschrieben.

Directory Groups: Dieses Eingabefeld benötigen Sie nur, wenn Sie eine Authentisierung mittels *Radius*, *LDAP* oder *Active Directory* einsetzen. Tragen Sie in dieser Spalte den **Gruppennamen** (**Group Name**) aus dem Verzeichnisdienst ein, dem dieses **Profil** (**Profile**) zugeteilt werden soll. Für *LDAP* tragen Sie hier bitte den **Distinguished Name** (**DN**) ein, der auf dem LDAP-Server auch zur Benutzerabfrage verwendet wird.
Wenn Sie *Active Directory* verwenden, müssen Sie für den Zugriff auf den HTTP-Proxy zusätzlich zu der *Gruppennamen* in diesem Feld eine Gruppe mit der Bezeichnung **http_access** definieren.

Assigned local Users: In diesem Feld wählen Sie den **lokalen Benutzer** aus, der diesem Profil zugewiesen werden soll.
Durch einen Klick auf das Feld mit dem Eintrag wird das Auswahlfeld geöffnet. Mit der Schaltfläche **Save** werden die Änderungen gespeichert. Durch einen Klick auf die Schaltfläche **Cancel** wird der alte Eintrag beibehalten.

Wichtiger Hinweis:

Wenn Sie einem **Profile** gleichzeitig einen **lokalen Benutzer** und ein **Netzwerk** zuweisen, dann wird das *Profile* nur wirksam, wenn der Benutzer auch aus dem „eingestellten“ Netzwerk auf den HTTP-Proxy zugreift! Einem lokalen Benutzer oder einem Netzwerk kann immer nur ein **Surf Protection Profile** zugeordnet werden.

Assigned Network Blocks: In diesem Feld wählen Sie das **Netzwerk** aus, der diesem Profil zugewiesen werden soll.
Durch einen Klick auf das Feld mit dem Eintrag wird das Auswahlfeld geöffnet. Mit der Schaltfläche **Save** werden die Änderungen gespeichert. Durch einen Klick auf die Schaltfläche **Cancel** wird der alte Eintrag beibehalten.

Surf Protection Profile zuweisen:

Per Default befindet sich in der Tabelle bereits eine **Blanko-Zuweisung** (**Blank Assignment**). Falls Diese Blanko-Zuweiung noch nicht editiert wurde, fahren Sie mit Schritt 2 fort.

1. Fügen Sie durch einen Klick auf die Schaltfläche **Add blank Assignment** eine neue Blanko-Zuweisung in die Tabelle ein.

2. Wählen Sie im Feld **Profile Name** das **Surf Protection Profile** aus.

3. Wählen Sie im Feld **Assigned local Users** den lokalen Benutzer für dieses Profile aus.

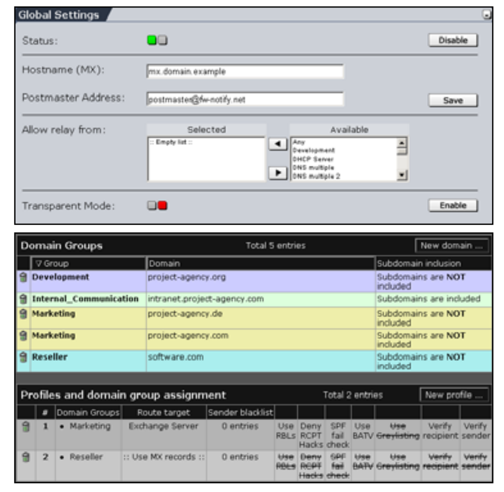
4. Wählen Sie im Feld **Assigned Network Blocks** das Netzwerk für dieses Profile aus.

5. Schalten Sie die Profile-Zuweisung durch einen Klick auf die **Statusampel** ein.

   Die Statusampel zeigt Grün.

Wenn nun ein Benutzer oder ein Rechner mit einem zugewiesenen Profile auf eine unerlaubte Internetseite zugreift, wird der Zugang nicht nur verhindert, sondern er erhält auch eine entsprechende Meldung.

5.6.2. SMTP



Mit dem **SMTP-Proxy** schützen Sie den internen Mail-Server vor Angriffen. Ein- und ausgehende E-Mails werden auf schädliche Inhalte überprüft. Sie können in diesem Menü auch *Spam-Protection*-Parameter eingeben, um unerwünschte E-Mails zu filtern.

In diesem Menü konfigurieren Sie den **SMTP-Proxy** für E-Mails. Der SMTP-Proxy empfängt alle E-Mails auf dem Gateway und versendet Sie im zweiten Prozess wieder. Damit werden keine Protokollbefehle weitergeleitet, sondern nur die Daten selbst. Der SMTP-Proxy setzt das SMTP-Protokoll auf dem TCP/IP-Port 25 um.

Der SMTP-Proxy kann auch im **Transparent-Modus** betrieben werden. Der große Vorteil von diesem Modus liegt in der erhöhten Sicherheit bei der Nutzung bestimmter Dienste, ohne dass dabei die Flexibilität verloren geht. Des Weiteren entsteht kein zusätzlicher Administrationsaufwand für Clients oder Server.

Wichtiger Hinweis:

Um eine einwandfreie Funktion des **SMTP**–Relay zu gewährleisten, muss ein gültiger **Nameserver (DNS)** aktiviert sein. Die **Firewall-Meldungen** (**Notifications**) an den Administrator werden auch bei abgeschaltetem **SMTP-Proxy** verschickt. Beachten Sie dazu auch die Beschreibung zur Einstellung **Route Target**.

SMTP-Proxy konfigurieren:

1. Öffnen Sie im Verzeichnis **Proxies** das Menü **SMTP**.
2. Schalten Sie den Proxy durch einen Klick auf die Schaltfläche **Enable** ein.
3. Führen Sie im Fenster **Global Settings** die Grundeinstellungen durch.

   Hostname (MX): Tragen Sie hier den Hostnamen ein.

   Wichtiger Hinweis:

   Wenn Sie TLS-Verschlüsselung verwenden möchten, muss dieser Hostname identisch sein mit dem in Ihrer DNS-Zone angegebenen **MX Record** (Mail Exchanger). Ansonsten werden andere SMTP-Server eventuell die Auslieferung von E-Mails mit TLS verweigern.

   Postmaster Address: Geben Sie hier die E-Mail-Adresse des Postmasters ein.
4. Speichern Sie die Eingaben durch einen Klick auf die Schaltfläche **Save**.
5. Wählen Sie im Fenster **Allow Relay from** die Netzwerke oder Hosts aus, die in der Lagen sein sollen, über den *SMTP-Proxy* E-Mails zu versenden.

   Sicherheitshinweis:

   Die Nachrichten, die von diesen Netzwerken aus versendet werden, werden von **Spam Protection** nicht gescant.

   Von den Hosts, die nicht im Auswahlfeld **Selected** enthalten sind, können nur E-Mails an die Domains versendet werden, die in der Tabelle **Domain Groups** definiert wurden.
6. Klicken Sie in der Zeile **Transparent Mode** auf die Schaltfläche **Enable**, wenn der Proxy in diesem Modus betrieben werden soll.

Anschließend zeigt die Statusampel grün.

Das Auswahlfeld **Skip source / destination networks** wird nur im Transparent-Modus angezeigt. Hier haben Sie die Möglichkeit bestimmte Netzwerke oder Hosts für den Proxy auszuschließen.

Die Funktionsweise des **Auswahlfeldes** wird in Kapitel 4.3.2 ab Seite 41 beschrieben.

Die Grundeinstellungen sind nun durchgeführt. Aus den eingestellten Netzwerken können nun über den Proxy E-Mails versendet werden.

Die Domain-Groups-Tabelle

In dieser Tabelle können mehrere Domains (z. B. mydomain.com, mydomain.de etc.) in einer Gruppe zusammengefasst werden. Für jede Domain, bzw. Sub-Domain wird in der Tabelle eine Zeile hinzugefügt. Die Zusammenfassung erfolgt über den Group-Namen.

Das nachfolgende Bild zeigt vier **Domain Groups**:

Domain Groups — Total 5 entries — New domain ...

	▽ Group	Domain	Subdomain inclusion
	Development	project-agency.org	Subdomains are **NOT** included
	Internal_Communication	intranet.project-agency.com	Subdomains are included
	Marketing	project-agency.de	Subdomains are **NOT** included
	Marketing	project-agency.com	Subdomains are **NOT** included
	Reseller	software.com	Subdomains are **NOT** included

Die Funktionen von links nach rechts sind:

Domain Group löschen ( ): Durch einen Klick auf das Papierkorb-Symbol wird die Domain-Gruppe aus der Tabelle gelöscht.

Group: Dies ist der Name der Gruppe. Dieser Group-Name wird benötigt, um der Domain in dieser Zeile ein bestimmtes Profil zuzuweisen.
Das Editierfenster wird durch einen Klick auf das Feld mit dem Eintrag (z. B. Default) geöffnet. Mit der Schaltfläche **Save** wird die Änderung gespeichert. Durch einen Klick auf die Schaltfläche **Cancel** wird der alte Eintrag beibehalten.

Domain: In dieses Feld wird die Domain eingetragen.
Das Editierfenster wird durch einen Klick auf das Feld mit dem Eintrag (z. B. Default) geöffnet. Mit der Schaltfläche **Save** wird die Änderung gespeichert. Durch einen Klick auf die Schaltfläche **Cancel** wird der alte Eintrag beibehalten.

Subdomain inclusion: Durch einen Klick auf die Meldung in dieser Spalte können die Sub-Domains in die Gruppe einbezogen werden.

Domain hinzufügen und editieren:

1. Um eine neue **Blanko-Domain** in die Tabelle einzufügen klicken Sie auf die Schaltfläche **New Domain**.

   Anschließend können Sie die *Domain*-Zeile editieren.

2. Tragen Sie in das Feld **Group** einen eindeutigen Namen für die Domain-Gruppe ein.

3. Definieren Sie in das Feld **Domain** die Domain ein.

4. Falls die Sub-Domains in die Gruppe einbezogen werden sollen, klicken Sie auf das Feld **Subdomain inclusion**.

Die Profiles-and-Domain-Group-Assignment-Tabelle

Das nachfolgende Bild zeigt zwei **Domain Profiles**:

Profiles and domain group assignment — Total 2 entries — New profile ...

	#	Domain Groups	Route target	Sender blacklist							
	1	• Marketing	Exchange Server	3 entries	Use RBLs	Deny RCPT Hacks	SPF fail check	Use BATV	~~Use Greylisting~~	Verify recipient	Verify sender
	2	• Reseller	:: Use MX records ::	0 entries	~~Use RBLs~~	~~Deny RCPT Hacks~~	~~SPF fail check~~	~~Use BATV~~	~~Use Greylisting~~	~~Verify recipient~~	~~Verify sender~~

Die Funktionen von links nach rechts sind:

Domain Groups: In diesem Feld wählen Sie den **Gruppennamen** (**Group Name**) aus der **Domain-Groups**-Tabelle aus.

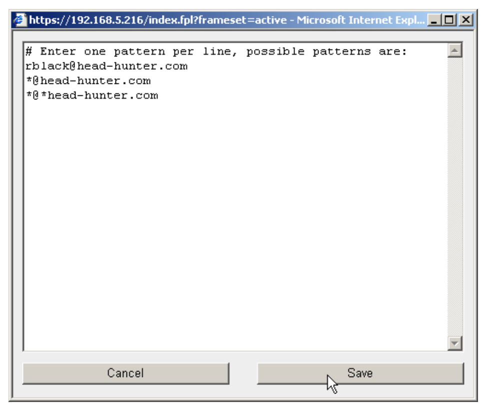
Route Target: Alle E-Mails für diese Domain-Gruppe müssen an einen bestimmten Host weitergeleitet werden. Übliche Hosts sind in diesem Fall z. B. der **Microsoft-Exchange-Server** oder **Lotus Notes**. Der Host muss zuvor im Menü **Definitions/Networks** definiert werden.

Sie können auch definieren, dass E-Mails an die angegebene Domain durch den MX-Record zugeschickt werden. Jedoch müssen Sie zuvor sicherstellen, dass die Firewall-IP-Adresse nicht selbst der primäre MX-Record der Domain ist, da sie keine E-Mails an sich selbst verschicken wird.

Wichtiger Hinweis:

Die statisch definierten Routen bleiben auch nach dem Ausschalten des *SMTP-Proxy* erhalten. Der *Mail Transfer Agent* **Exim** ist in diesem Fall von außerhalb der Firewall nicht mehr erreichbar. *Exim* wird allerdings weiterhin ausgeführt und versucht E-Mails, unter anderem auch die **Notifications**, über die statische Route weiterzuleiten. Bevor Sie den *SMTP-Proxy* ausschalten, sollten Sie daher die statischen Routen löschen oder die geänderte Route eintragen.

Sender Blacklist: Mit dieser Funktion können E-Mails mit bestimmten Absenderadressen, z. B. von bekannten Spam-Hosts geblockt werden. Beide Absenderadressen auf dem Umschlag sowie die "*From:*"- und "*Reply-To:*"-*Header* der eingehenden E-Mails werden mit der Kontrollliste verglichen.



Tragen Sie die Adressen wie nachfolgend beschrieben in die Kontrollliste ein. Die Kontrollliste wird durch einen Klick auf die Meldung (z. B. 0 entries) geöffnet:

- E-Mails einer bestimmten Adresse sollen geblockt werden.
  Eingabe: user@domain.com
- Alle E-Mails einer bestimmten Domain sollen geblockt werden.
  Eingabe: *@*domain.com
- Alle E-Mails eines bestimmten Benutzers sollen blockiert werden, egal von welcher Domain diese abgesendet werden.
  Eingabe: user@*

Kommentare müssen durch das Zeichen **#** am Anfang jeder Zeile gekennzeichnet werden. Adressen, die mit diesem Zeichen beginnen, werden von der Funktion *Sender Blacklist* nicht berücksichtigt!

Mit der Schaltfläche **Save** werden die Änderungen gespeichert. Durch einen Klick auf die Schaltfläche **Cancel** wird der alte Eintrag beibehalten.

Die Anzahl der Patterns wird anschließend im Feld angezeigt. Wenn die Firewall nun eine E-Mail von einer Adresse aus der Kontrollliste empfängt, wird diese mit der Fehlermeldung **5xx** und dem Kommentar **Your address (envelope or header) is blacklisted at this site** zurückgesendet.

Use RBL: Mit der Funktion **Realtime Blackhole Lists** (**RBL**) können externe Datenbanken mit den Ihnen bekannten Spam-Hosts abgefragt werden. Die E-Mails, die von einer Domain aus der Datenbank in der Kontrollliste zugesendet wurden, werden zurückgewiesen (Aktion: Reject). Im Internet werden mehrere Dienste dieser Art angeboten. Durch diese Funktion kann der Umfang an unerwünschten E-Mails stark reduziert werden.

In der Kontrollliste sind bereits Datenbanken vordefiniert. Diese Datenbanken werden von **Astaro** nur empfohlen. **Astaro** übernimmt keine Gewähr für den Inhalt dieser Datenbanken.

Einen weiteren kommerziellen Dienst finden Sie unter der Internetadresse http://www.mail-abuse.com.

Die Internetadressen der Datenbanken werden im Fenster **Feature Settings** in die Kontrollliste **RBL Zones** eingetragen.

Die Funktionsweise der **Kontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.5 ab Seite 43 beschrieben.

Deny RCPT Hacks: Der Proxy akzeptiert keine E-Mails die eine Absenderadresse mit den Zeichen **!**, **%**, **/**, **|** oder einem zusätzlichen **@** enthält. Des Weiteren werden auch E-Mails nicht akzeptiert, die mit einem **Dot** (**.**) beginnen.

SPF Fail Check: Mit dieser Funktion prüft die Firewall anhand von Sender Policy Framework (SPF) ob die eingehenden E-Mails vom richtigen Server aus versendet wurden. SPF wird durch spezielle DNS-Einträge zur Verfügung gestellt, die hier abgefragt werden. Durch *SPF* haben die Inhaber von Domains so die Möglichkeit Informationen zu ihren Mail-Servern im DNS zu veröffentlichen.
Eine Domain verwendet öffentliche **Records** (**DNS**) um Anfragen zu den verschiedenen Diensten (z. B. HTTP, SMTP, etc.) an Rechner zu richten, die diese Dienste ausführen. Die **Mail (MX) Records** werden bereits von allen Domains veröffentlicht, um die anderen darüber zu informieren, welche Rechner E-Mails für diese Domain erhalten. Durch **SPF** werden nun die „entgegengesetzten“ **Mail (MX) Records** veröffentlicht, in denen mitgeteilt wird, welche Rechner E-Mails von einer bestimmten Domain aus versenden. Der Empfänger einer Mail kann nun diese *Records* prüfen und feststellen, ob diese auch wirklick von dieser Domain abgeschickt wurde.

Use BATV: Bei der Funktion **Bounce Address Tag Validation** (**BATV**) handelt es sich um ein Tool des Standardisierungsgremiums **Internet Engineering Task Force** (**IETF**). Mittels Domain Keys sollen die *Internet Service Provider* (*ISP*) in der Lage sein unerwünschte Massen-Mails leichter zu blockieren, indem verhindert wird, dass die Absenderadresse der E-Mail verschleiert oder gefälscht wird. Durch die Funktion **BATV** wird den ausgehenden E-Mails eine verschlüsselte digitale Signatur angehängt, die den Server des Absenders anzeigt.

Anhand der auf dieser Firewall in Quarantäne genommenen E-Mails werden Sie festellen, dass es sich bei 40% der *Spam Mails* um *Bounce Mails* handelt. Durch die angehängte Signatur kann das System nun feststellen, ob die *Bounce Mail*, die Sie erhalten haben, ursprünglich durch Ihre E-Mail verursacht wurde und nicht durch einen Versender von *Spam Mails*, der die Absenderadresse gefälscht hat. Diese Art von *Spam Mails* kann von der Firewall immer ohne die Gefahr eines Fehlalarms zurückgewiesen werden. Hinzu kommt, dass durch die Funktion grundsätzlich alle E-Mails abgewiesen werden, die keine Absenderadresse enthalten.
Bitte beachten Sie, dass die durch **BATV** erzeugten Signaturen nach sieben Tagen ungültig werden!

Im Fenster **Feature Settings** können zur Funktion **BATV** zusätzliche Einstellungen vorgenommen werden.

Use Greylisting: Ein Mail-Server, der mit **Greylisting** arbeitet, speichert in der Regel von eingehenden E-Mails die folgenden drei Informationen in einem sogenannten **Triplet**:

- Die Absenderadresse
- Die IP-Adresse des Absenders
- Die Empfängeradresse

Das *Triplet* wird nun mit der internen Datenbank des SMTP-Proxy verglichen. Wenn dieses *Triplet* noch nicht vorhanden ist, wird es in der Datenbank angelegt und erhält einen speziellen Zeitstempel. Aufgrund dieses Zeitstempels wird die E-Mail vom SMTP-Proxy für den Zeitraum von fünf Minuten abgelehnt. Diese Aktion wird als *Greylisting* bezeichnet. Nach dieser Zeitspanne gilt das *Triplet* als bekannt und die Mail wird beim nächsten Zustellversuch akzeptiert.
Das *Greylisting* nutzt die Tatsache, dass die meisten Versender von *Spam Mails* Software verwenden, die nach der *Fire-and-Forget*-Methode arbeiten: Versuche die E-Mail zuzustellen und wenn es nicht klappt, vergiss es! Das heißt, dass die Versender solcher Spams nicht wie RFC-konforme Mail-Server versuchen die Mail bei einem *Tempo-*

rary Failure nochmals zu versenden.
Wenn der Zeitstempel älter als fünf Minuten ist, wird die E-Mail sofort verschickt und seine Gültigkeit wird mit der aktuellen Uhrzeit minus fünf Minuten aktualisiert.

Verify Recipient: Mit dieser Funktion werden die Empfängeradressen von ankommenden E-Mails mit den Adressen auf Ihrem Backend Mail Server verglichen. Damit dies funktioniert, muss der Backend Mail Server E-Mails an unbekannte Empfängeradressen auf SMTP-Ebene zurückweisen! Die allgemeingültige Regel lautet: Wenn der Backend Mail Server die Nachricht zurückweist, dann wird Sie auch von der Firewall zurückgewiesen.

Verify Sender: Mit dieser Funktion werden die Absenderadressen von ankommenden E-Mails überprüft. Es wird geprüft, ob von der Absenderadresse tatsächlich Nachrichten zugestellt werden können, indem eine Verbindung zum Host aufgebaut und ein RCPT-Befehl ausgeführt wird. Falls dies nicht der Fall ist, wird die E-Mail zurückgewiesen.

Domain Profile editieren:

1. Um ein neues **Blanko-Profile** in die Tabelle einzufügen klicken Sie auf die Schaltfläche **New Profile**.

   Anschließend können Sie die *Profile*-Zeile editieren.

2. Wählen Sie für die eingehenden E-Mails im Feld **Domain Groups** die Gruppe aus der Tabelle **Domain Groups** aus.

   Das Auswahlfenster wird durch einen Klick auf die Meldung (z. B. empty) geöffnet.

3. Definieren Sie im Feld **Route Target** die Route für die eingehenden E-Mails.

   Das Auswahlfenster wird durch einen Klick auf die Meldung (z. B. use MX records) geöffnet.

Alle E-Mails für diese Domain-Gruppe müssen an einen bestimmten Host weitergeleitet werden. Übliche Hosts sind in diesem Fall z. B. der **Microsoft Exchange Server** oder **Lotus Notes**. Der Host muss zuvor im Menü **Definitions/Networks** definiert werden.

Sie können auch definieren, dass E-Mails an die angegebene Domain durch den MX-Record zugeschickt werden. Jedoch müssen Sie zuvor sicherstellen, dass die Firewall-IP-Adresse nicht selbst der primäre MX-Record (Use MX records) der Domain ist, da sie keine E-Mails an sich selbst verschicken wird.

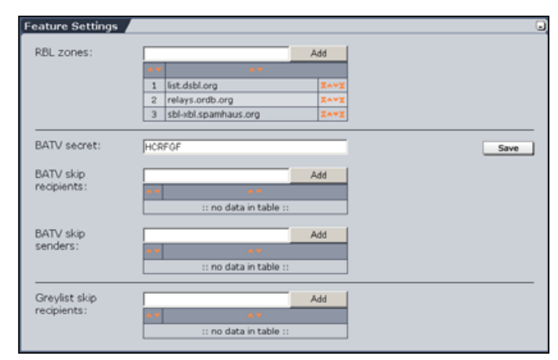
Beachten Sie, dass die hier statisch eingetragenen Routen auch nach dem Ausschalten des SMTP-Proxy erhalten bleiben.

4. Stellen Sie in den weiteren Spalten die **Spam-Protection**-Funktionen für dieses Profil ein.

   Die Funktionen werden im Abschnitt **Die Profiles-and-Domain-Group-Assignment-Tabelle** beschrieben.

Das **Domain Profile** ist nun einer Domaingruppe zugewiesen und ediert. Die Einstellungen werden sofort ohne einer weiteren Bestätigung wirksam.

Feature Settings



Im Fenster **Feature Settings** befinden sich die Zusatzeinstellungen für die **Spam-Protection**-Funktionen in der Tabelle **Profiles and Domain Group Assignment**.

RBL Zones: Tragen Sie in diese Kontrollliste die Internetadressen der Datenbanken für die Funktion **Use RBL** ein.

Die Funktionsweise der **Kontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.5 ab Seite 43 beschrieben.

BATV Secret: Der automatisch generierte **Security Key** kann auch manuell definiert werden. Wenn Sie mehrere Firewalls als MX einsetzen, muss auf allen Systemen der gleiche *Security Key* eingetragen werden.

BATV skip Recipients: In diese Kontrollliste können Sie Empfänger eintragen, an die unsignierte Nachrichten abgeschickt werden sollen. Dies ist z. B. notwendig, wenn Nachrichten über einen Verteiler zugestellt werden, für den die Umschlagsabsenderadresse benötigt wird. Der Nachteil ist, dass Ihnen von den Adressen in der Kontrollliste keine Bounce-Nachrichten zugestellt werden.

BATV skip Senders: In diese Kontrollliste können Sie die Adressen eintragen, von denen aus unsignierte Nachrichten verschickt werden sollen.

Greylist skip Recipients: In diese Kontrollliste können Sie die Empfänger eintragen, die von der Funktion *Greylisting* ausgenommen werden sollen.

5.6.2.1. Content Filter

Content Filter

Scan outgoing messages:	Disable
MIME Error Checking:	Enable
File Extension Filter:	Enable
Virus Protection:	Enable
Expression Filter:	Enable

Scan outgoing Messages

Die Funktion **Scan Outgoing Messages** wendet den **Content Filter** auf die ausgehenden Verbindungen an.

MIME Error Checking

Die Funktion **MIME Error Checking** kann Fehler in Nachrichten erkennen, die mit **MIME** verschlüsselt wurden. **MIME** steht für **M**ultipurpose **I**nternet **M**ail **E**xtensions. MIME legt die Struktur und den Aufbau von E-Mails und anderer Internetnachrichten fest. Es ist eine Kodierungsvorschrift, die den Versand von Nicht-Text-Dokumenten, wie Bilder, Audio und Video in textbasierten Übertragungssystemen ermöglicht. Die Nicht-Text-Elemente werden beim Versender verschlüsselt und beim Empfänger wieder entschlüsselt.

Die Funktion **MIME Error Checking** kann dabei helfen Angriffe, bei denen die Fehler-Toleranzabweichung in der MIME-Entschlüsselungs-Software ausgenutzt werden zu erkennen.

Action: In diesem Drop-down-Menü legen Sie fest, wie eine von der Firewall gefilterte E-Mail behandelt wird. Folgende Aktionen sind möglich:

- **Reject**: Die E-Mail wird mit der Fehlernummer **5xx** und einem Kommentar abgewiesen. Die Bounce-Nachricht an den Absender enthält auch eine Begründung, warum die E-Mail blockiert wurde.
- **Blackhole**: Die E-Mail wird angenommen und sofort gelöscht. Diese Aktion sollten Sie nur verwenden, wenn Sie absolut sicher sind.
- **Quarantine**: Die E-Mail wird angenommen, kommt aber in Quarantäne. Die E-Mail wird im Menü **Proxy Content Manager** mit dem Status **Quarantine** angezeigt. In diesem Menü stehen Ihnen weitere Funktionen zur Verfügung, um die E-Mail z. B. sicher zu lesen oder zu versenden.
- **Warn**: Die E-Mail wird vom Filter behandelt aber durchgelassen. Der E-Mail wird aber ein **Header** hinzugefügt, der es ermöglicht diese auf dem Mail-Server oder im E-Mail-Programm des Empfängers zu sortieren oder zu filtern.

  Wie in **Microsoft Outlook 2000** die Regeln erstellt werden wird auf Seite 325 beschrieben.

Trigger on: In diesem Drop-down-Menü legen Sie fest, welche Fehler dazu führen, dass die E-Mail laut Funktion Action behandelt wird:

- **Level 1**: Diese Stufe bewirkt, dass nur die E-Mails mit den schwersten Fehlern behandelt werden. Diese Einstellung wird empfohlen, da viele Anwender ein fehlerhaftes Verschlüsselungsprogramm verwenden, das bei den höheren Stufen (Level 2 und 3) bereits anspricht.
- **Level 2**: Mit Ausnahme der mit alltäglichen Fehlern behafteten E-Mails, werden alle behandelt.
- **Level 3**: Alle E-Mails mit Fehlern werden behandelt.

File Extension Filter

Mit dieser Funktion filtert die Firewall die Anhänge (Attachments) mit den Erweiterungen aus der Kontrollliste **Extensions**.

Action: In diesem Drop-down-Menü legen Sie fest, wie eine von der Firewall gefilterte E-Mail behandelt wird. Folgende Aktionen sind möglich:

- **Reject**: Die E-Mail wird mit der Fehlermeldung **5xx** und einem Kommentar zurückgesendet. Aufgrund dieses Kommentars wird der Host, der diese E-Mail versendet hat, wiederum eine Bounce-Nachricht an die Absenderadresse schicken.
- **Blackhole**: Die E-Mail wird angenommen und sofort gelöscht. Diese Aktion sollten Sie nur verwenden, wenn Sie absolut sicher sind.
- **Quarantine**: Die E-Mail wird angenommen, kommt aber in Quarantäne. Die E-Mail wird im Menü **Proxy Content Manager** mit dem Status **Quarantine** angezeigt. In diesem Menü stehen Ihnen weitere Funktionen zur Verfügung, um die E-Mail z. B. sicher zu lesen oder zu versenden.
- **Warn**: Die E-Mail wird vom Filter behandelt aber durchgelassen. Der E-Mail wird aber ein **Header** hinzugefügt, der es ermöglicht diese auf dem Mail-Server oder im E-Mail-Programm des Empfängers zu sortieren oder zu filtern.

  Wie in **Microsoft Outlook 2000** die Regeln erstellt werden wird auf Seite 325 beschrieben.

Extensions: Tragen Sie in die Kontrollliste alle Dateierweiterungen ein (z. B. **exe**), die von der Firewall gefiltert werden sollen.

Die Funktionsweise der **Kontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.5 ab Seite 43 beschrieben.

Virus Protection

Mit dem Modul **Virus Protection** werden E-Mails und Anhänge (Attachments) auf gefährliche Inhalte, z. B. Viren und Trojanische Pferde untersucht. Der Scanvorgang wird im E-Mail-Header vermerkt.

Falls **Virus Protection** eine infizierte E-Mail entdeckt, wird diese von der Firewall gefiltert. Die weitere Behandlung der E-Mail hängt von der Einstellung im Drop-down-Menü **Action** ab.

Action: In diesem Drop-down-Menü legen Sie fest, wie eine von der Firewall gefilterte E-Mail behandelt wird. Folgende Aktionen sind möglich:

- **Reject**: Die E-Mail wird mit der Fehlermeldung **5xx** und einem Kommentar zurückgesendet. Aufgrund dieses Kommentars wird der Host, der diese E-Mail versendet hat, wiederum eine Bounce-Nachricht an die Absenderadresse schicken.
- **Blackhole**: Die E-Mail wird angenommen und sofort gelöscht.
- **Quarantine**: Die E-Mail wird angenommen, kommt aber in Quarantäne. Die E-Mail wird im Menü **Proxy Content Manager** mit dem Status **Quarantine** angezeigt. In diesem Menü stehen Ihnen weitere Funktionen zur Verfügung, um die E-Mail z. B. sicher zu lesen.
- **Warn**: Die E-Mail wird vom Filter behandelt aber durchgelassen. Der E-Mail wird aber ein **Header** hinzugefügt, der es ermöglicht diese auf dem Mail-Server oder im E-Mail-Programm des Empfängers zu sortieren oder zu filtern.

  Wie in **Microsoft Outlook 2000** die Regeln erstellt werden wird auf Seite 325 beschrieben.

Expression Filter

Es besteht auch die Möglichkeit, dass neue Viren der Firewall noch nicht bekannt sind. Diese Viren können aber auch aufgrund einer bekannten Zeichenkette, z. B. der I-love-you-Virus, erkannt werden. Die Zeichenketten werden in die Kontrollliste eingegeben. Wenn nun eine E-Mail diese Zeichenkette enthält, wird sie blockiert.
Neben einfachen Zeichenketten können auch Ausdrücke in Form von **Perl Compatible Regular Expressions** definiert werden.

Action: In diesem Drop-down-Menü legen Sie fest, wie eine von der Firewall gefilterte E-Mail behandelt wird. Folgende Aktionen sind möglich:

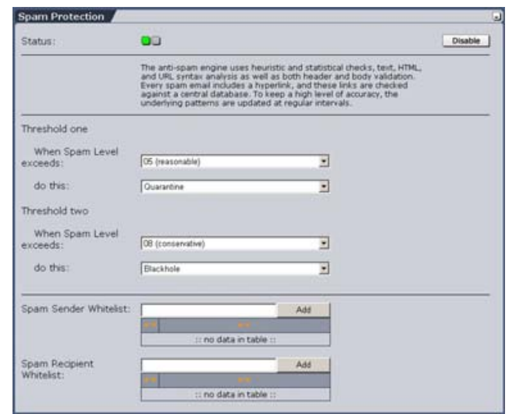
- **Reject**: Die E-Mail wird mit der Fehlermeldung **5xx** und einem Kommentar zurückgesendet. Aufgrund dieses Kommentars wird der Host, der diese E-Mail versendet hat, wiederum eine Bounce-Nachricht an die Absenderadresse schicken.
- **Blackhole**: Die E-Mail wird angenommen und sofort gelöscht.
- **Quarantine**: Die E-Mail wird angenommen, kommt aber in Quarantäne. Die E-Mail wird im Menü **Proxy Content Manager** mit dem Status **Quarantine** angezeigt. In diesem Menü stehen Ihnen weitere Funktionen zur Verfügung, um die E-Mail z. B. sicher zu lesen oder zu versenden.
- **Warn**: Die E-Mail wird vom Filter behandelt aber durchgelassen. Der E-Mail wird aber ein **Header** hinzugefügt, der es ermöglicht diese auf dem Mail-Server oder im E-Mail-Programm des Empfängers zu sortieren oder zu filtern.

  Wie in **Microsoft Outlook 2000** die Regeln erstellt werden wird auf Seite 325 beschrieben.

Expressions: Tragen Sie in die Kontrollliste die Zeichenketten ein.

Die Funktionsweise der **Kontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.5 ab Seite 43 beschrieben.

5.6.2.2. Spam Protection



Dieses Modul überprüft die eingehenden E-Mails heuristisch auf bestimmte Eigenschaften die Hinweise auf Spam geben. Hierzu dienen interne Musterdatenbanken. Auf diese Weise ist man unabhängig von den Absenderinformationen und kann somit die Genauigkeit stark erhöhen.

Wichtiger Hinweis:

Wenn Sie eine Upstream Firewall einsetzen, müssen Sie dort den Datenverkehr vom Sicherheitssystem zum Internet durch den nachfolgend aufgeführten Port erlauben. Er wird für die Kommunikation mit der **Spam-Protection**-Datenbank benötigt: UDP Port 53 (DNS).

Für den *Spam Score* können zwei **Grenzwerte** (**Thresholds**) definiert werden. Auf diese Weise können mutmaßliche Spam E-Mails von der Firewall unterschiedlich behandelt werden.
Die beiden **Grenzwerte** (**Thresholds**) sind gleichberechtigt. Der Grenzwert mit der höheren Stufe sollte allerdings strenger behandelt werden. Die Funktionsweise wird weiter unten anhand der Default-Einstellungen erläutert.

Default-Einstellungen:

Grenzwert Eins (**Threshold One**)

When Spam Level exceeds: 05 (reasonable),
do this: Quarantine.

Grenzwert Zwei (**Threshold Two**)

When Spam Level exceeds: 08 (conservative),
do this: Reject.

Der erste Grenzwert hat zur Folge, dass E-Mails ab Stufe 5 gefiltert und in Quarantäne kommt. Die E-Mail wird im Menü **Proxy Content Manager** mit dem Status **Quarantine** angezeigt.
Beim zweiten Grenzwert wird die E-Mail mit einem Kommentar zurückgesendet.

Grundsätzliche gilt, dass der **Grenzwert** (**Threshold**) mit der höheren Stufe eine strengere Behandlung (**do this**) erfahren soll.

Wichtiger Hinweis:

Das Modul **Spam Protection** benötigt auf stark frequentierten Systemen einen hohen Anteil der Systemressourcen.

When Spam Level exceeds: Mit diesem Drop-down-Menü justieren Sie den Höchstwert zur Bewertung der E-Mails. Der Unterschied zwischen den Höchstwerten definiert sich durch die Wahrscheinlichkeit, dass ungefährliche Mails, z. B. HTML-Newsletter gefiltert werden. Im Drop-down-Menü kann ein Wert zwischen 1 und 15 eingestellt werden. Mit der Stufe 1 werden bereits E-Mails mit einem kleinen *Spam Score* behandelt. Die folgenden Stufen (Level) geben einen Anhaltspunkt:

- **Aggressive (03)**: Diese Strategie filtert die meisten Spam-Mails. Allerdings werden mit hoher Wahrscheinlichkeit auch ungefährliche Nachrichten, z. B. HTML-Newsletter zurückgewiesen.
- **Reasonable (05)**: Diese Strategie liegt zwischen **Aggressive** und **Conservative**.
- **Conservative (08)**: Diese Strategie filtert nur Nachrichten, bei denen es sich mit sehr hoher Wahrscheinlichkeit um Spam-Mails handelt. Ungefährliche E-Mails werden meist nicht gefiltert.

do this: In diesem Drop-down-Menü legen Sie fest, wie eine von der Firewall gefilterte E-Mail behandelt wird. Folgende Aktionen sind möglich:

- **Reject**: Die E-Mail wird mit der Fehlernumer **5xx** und einem Kommentar zurückgesendet. Aufgrund dieses Kommentars wird der Host, der diese E-Mail versendet hat, wiederum eine Bounce-Nachricht an die Absenderadresse schicken.
- **Blackhole**: Die E-Mail wird angenommen und sofort gelöscht. Diese Aktion sollten Sie nur verwenden, wenn Sie absolut sicher sind.
- **Quarantine**: Die E-Mail wird angenommen, kommt aber in Quarantäne. Die E-Mail wird im Menü **Proxy Content Manager** mit dem Status **Quarantine** angezeigt. In diesem Menü stehen Ihnen weitere Funktionen zur Verfügung, um die E-Mail z. B. sicher zu lesen oder zu verenden.
- **Warn**: Die E-Mail wird vom Filter behandelt aber durchgelassen. Der E-Mail wird aber ein **Header** hinzugefügt, der es ermöglicht diese auf dem Mail-Server oder im E-Mail-Programm des Empfängers zu sortieren oder zu filtern. Des Weiteren wird in den Betreff der E-Mail der Hinweis ***SPAM*** hinzugefügt.

  Wie in **Microsoft Outlook 2000** die Regeln erstellt werden wird auf Seite 325 beschrieben.

Spam Sender Whitelist: Mit dieser Kontrollliste können die E-Mails bestimmter Absender vom Scannvorgang durch das Modul **Spam Protection** ausgeschlossen werden. Es werden alle Nachrichten nicht gescannt, in denen die "*Envelope-from*"-Adresse oder "*Header*"-Absender mit einem Eintrag aus der Kontrollliste übereinstimmen.

Tragen Sie die Adressen wie nachfolgend beschrieben in die Kontrollliste ein:

- E-Mails einer bestimmten Adresse sollen nicht gescannt werden. Eingabe: user@domain.com
- Alle E-Mails einer bestimmten Domain sollen nicht gescannt werden. Eingabe: *@*domain.com
- Alle E-Mails eines bestimmten Benutzers sollen nicht gescannt werden, egal von welcher Domain diese abgesendet werden. Eingabe: user@*

Die Funktionsweise der **Kontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.5 ab Seite 43 beschrieben.

Spam Recipient Whitelist: Mit dieser Kontrollliste können die E-Mails für bestimmte Empfänger vom Scannvorgang durch das Modul **Spam Protection** ausgeschlossen werden. Es werden alle Nachrichten nicht gescannt, in denen die "*Envelope recipient*"-Adresse mit einem Eintrag aus der Kontrollliste übereinstimmen.

Tragen Sie die Adressen wie nachfolgend beschrieben in die Kontrollliste ein:

- Nachrichten für eine bestimmte E-Mail-Adresse sollen nicht gescannt werden. Eingabe: user@domain.com
- Alle E-Mails an eine bestimmte Domain sollen nicht gescannt werden. Eingabe: *@*domain.com
- Alle E-Mails an einen bestimmten Benutzer sollen nicht gescannt werden. Eingabe: user@*

Die Funktionsweise der **Kontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.5 ab Seite 43 beschrieben.

Die Header

Bei einigen **Content-Filter**-Funktionen wird der gescannten Nachricht ein **Header** hinzugefügt. Dieser Header soll den Benutzer über spezielle Eigenschaften dieser Nachricht informieren. Wenn nun bei der entsprechenden Funktion die Aktion **Warn** (SMTP) oder **Pass** (POP3) ausgewählt wird, können die Empfänger verdächtige Nachrichten mit ihrer E-Mail-Software sortieren oder filtern. In der nachfolgenden Liste sind alle Header enthalten, die der SMTP-Proxy an die E-Mails hinzufügen kann:

- **X-Spam-Score**: Dieser Header wird vom Modul **Spam Protection** hinzugefügt. Er enthält einen Punktestand, der aus einem numerischen Wert und einer Anzahl von Minus- und Pluszeichen besteht. Je höher dieser Punktestand ausfällt, umso wahrscheinlicher ist es, dass es sich bei der Nachricht um eine Spam-Mail handelt.
  Wenn Sie beim Modul **Spam Protection** die Aktion **Warn** auswählen, kann der Empfänger die E-Mail mit seiner E-Mail-Software filtern.
- **X-Spam-Flag**: Wenn der enthaltene Wert **Yes** lautet, wurde die Nachricht als Spam-Mail erkannt.
- **X-Spam-Report**: Der Proxy hat die Nachricht als Spam-Mail erkannt. Der hinzugefügte Multiline Header enthält einen offen lesbaren Antispam-Bericht.
- **X-Infected**: Die Nachricht enthält einen Virus. Als Wert wird der Name des gefundenen Viruses angezeigt.
- **X-Contains-File**: Dieser Header wird von der Funktion **File Extension Filter** hinzugefügt. Eine E-Mail enthält einen Anhang (Attachment) mit einer potentiell gefährlichen Erweiterung aus der Kontrollliste.
- **X-Regex-Match**: Dieser Header wird von der Funktion **Expression Filter** hinzugefügt. Die E-Mail beinhaltet eine Zeichenkette

aus der Kontrollliste.

In Microsoft Outlook 2000 Regeln erstellen:

In **MS Outlook** können die von der Firewall gescannten und anschließend durchgelassenen E-Mails anhand der **Header** sortiert werden. Voraussetzung hierfür ist, dass bei der entsprechenden **Content-Filter**-Funktion auf der Firewall die Aktion **Warn** (SMTP) oder **Pass** (POP3) ausgewählt wurde. Die verfügbaren Header sind auf der vorhergehenden Seite aufgelistet.

1. Starten Sie **MS Outlook**.
2. Klicken Sie auf **Posteingang**.
3. Öffnen Sie das Menü **Extras/Regel-Assistent**.
4. Klicken Sie auf die Schaltfläche **Neu**.

   Anschließend öffnet sich der Assistent zur Erstellung neuer Regeln. Dieser Regel-Assistent führt Sie nun schrittweise durch die Konfiguration.
5. Welche Art von Regel möchten Sie erstellen? (Schritt 1)

   Wählen Sie die Regel **Nachricht bei Ankunft prüfen** aus.

   Klicken Sie anschließend auf die Schaltfläche **Weiter**.
6. Welche Bedingung(en) möchten Sie überprüfen? (Schritt 2)

   Wählen Sie in diesem Fenster die Bedingung **mit bestimmten Wörtern in der Nachrichtenkopfzeile** aus.

   Klicken Sie im Fenster **Regelbeschreibung** auf den unterstrichenen Textabschnitt und tragen Sie in das Eingabefeld **Text suchen** den Namen des Headers ein. Beispiel: **X-Infected**

   Klicken Sie anschließend auf die Schaltfläche **Weiter**.
7. Was soll mit dieser Nachricht passieren? (Schritt 3)

   Definieren Sie in diesem Fenster, was mit der gefilterten E-Mail passieren soll. Falls z. B. die gefilterten E-Mails in einen be-

stimmten Zielordner verschoben werden sollen, wählen Sie die Aktion **diese in den Ordner Zielordner verschieben** aus.

Durch einen Klick auf **Zielordner** im Fenster **Regelbeschreibung** öffnet sich ein neues Menü. Hier können Sie entweder einen vorhanden Ordner auswählen oder einen neuen Zielordner für die gefilterten E-Mails erstellen. Beispiel: **Virus**
Speichern Sie in diesem Menü die neuen Einstellungen durch einen Klick auf die Schaltfläche **OK**.

Klicken Sie anschließend auf die Schaltfläche **Weiter**.

8. Ausnahme hinzufügen (Schritt 4)

In diesem Menü können Sie Ausnahmen definieren und so E-Mails, z. B. Nachrichten eines bestimmten Absenders, von dieser Regel ausschließen.

Klicken Sie anschließend auf die Schaltfläche **Weiter**.

9. Geben Sie einen Namen für die Regel ein (Schritt 5)

Tragen Sie in das Eingabefeld einen eindeutigen Namen für diese Regel ein. Mit den darunter liegenden Optionsfeldern können Sie diese Regel **aktivieren** und auch auf E-Mails anwenden, die sich bereits im Ordner **Posteingang** befinden. Im Fenster Regelbeschreibung können Sie Ihre Einstellungen ändern.

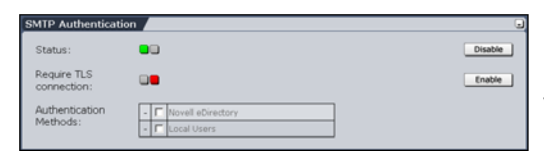
Klicken Sie anschließend auf die Schaltfläche **Fertig stellen**.

10. Regeln in dieser Reihenfolge anwenden (Schritt 6)

Im Regel-Assistenten können Sie die Regeln durch einen Klick auf das Optionsfeld aktivieren und deaktivieren sowie Änderungen durchführen.

Um den Regel-Assistenten zu schließen klicken Sie auf die Schaltfläche **OK**.

SMTP Authentication



Mit **SMTP Authentication** können sich Mail-Clients, wie z. B. MS Outlook, Outlook Express oder Netscape Messenger am **SMTP-Proxy** authentifizieren. Dies ist für dynamische IP-Endpunkte sehr nützlich. Mit der Funktion **Require TLS Connection** können Sie bestimmen, ob eine entsprechend verschlüsselte Verbindung benötigt wird. Für eingehende Verbindungen ist TLS immer eingeschaltet und der Proxy nutzt automatische die starke Verschlüsselung, wenn der externe Host diese Funktion unterstützt. SMTP ist normalerweise unverschlüsselt und kann von Dritten leicht mitgelesen werden. Die Funktion sollte aus diesem Grund möglichst eingeschaltet werden.

Wichtiger Hinweis:

Einige Mail-Server, z. B. Lotus Domino, haben teilweise Fehler in ihrer **TLS**-Konfiguration. Diese Mail-Server kündigen beim Verbindungsaufbau TLS an, obwohl sie durch eine unvollständige Konfiguration nicht in der Lage sind, eine TLS-Sitzung aufzubauen. Wenn TLS eingeschaltet ist, können keine E-Mails an diese Server verschickt werden. Bitte kontaktieren Sie in solch einem Fall die Administratoren dieser Mail-Server.

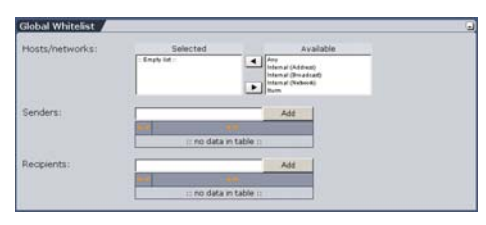
Bitte verwenden Sie in den SMTP-Authentifizierungseinstellungen des Clients nicht die Funktion SPA (Secure Password Authentication). Dies ist eine alternative Verschlüsselungsmethode, die von der Firewall nicht unterstützt wird. Verwenden Sie stattdessen eine unverschlüsselte Authentifizierungsmethode, und schalten zusätzlich für ausgehende E-Mails das TLS (oder SSL) Protokoll ein.

Mit dem Auswahlfeld **Authentication Methods** bestimmen Sie die Methode zur Benutzerauthentifizierung. Zur Auswahl stehen nur Authentifizierungsmethoden, die Sie zuvor im Menü **System / User**

Authentication konfiguriert haben.

Die lokalen **Benutzer (Users)** werden im Menü **Definitions/Users** verwaltet.

Global Whitelist



Mit dem Auswahlfeld kann eine **Global Whitelist** mit vertrauenswürdigen Hosts oder Netzwerken definiert werden, die in diesem Fall von den folgenden Funktionen ausgeschlossen werden:

- Virus Protection
- Spam Protection
- MIME Error Checking
- Expression Filter
- Sender Address Verification
- Realtime Blackhole Lists (RBL)
- Greylisting

Dies hat zur Folge, dass die benötigte Rechenleistung für Scanvorgänge herabgesetzt wird und dass problematische Hosts vom Content Scanning ausgeschlossen werden können.

Senders: mit der Kontrollliste können vertrauenswürdige Absenderadressen vom Content Scanning ausgeschlossen werden.

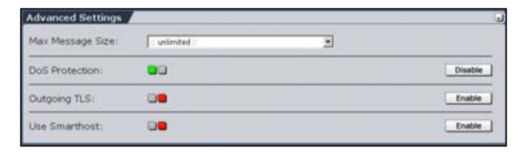


Sicherheitshinweis:

Diese Funktion sollte allerdings nur mit Vorsicht eingesetzt werden, da Absenderadressen auch leicht gefälscht werden können. Nutzen Sie möglichst das Auswahlfeld **Hosts/Networks**.

Recipients: mit der Kontrollliste können vertrauenswürdige Empfängeradressen vom Content Scanning ausgeschlossen werden.
Bitte beachten Sie, dass E-Mails mit mehreren Adressaten ebenfalls vom Content Scanning ausgeschlossen werden, wenn eine von diesen Adressen in der Kontrollliste enthalten ist.

Advanced Settings



Max Message Size: Hier stellen Sie die maximale Dateigröße für die ein- und ausgehenden E-Mails ein. Übliche Werte sind 20 oder 40 MB. Bitte beachten Sie, dass durch die Kodierungsverfahren an E-Mails angehängte Dateien wesentlich größer werden können.

DoS Protection: Um **Denial-of-Service-(DoS)**-Attacken vorzubeugen, werden bis zu 20 gleichzeitig eingehende SMTP-Verbindungen bearbeitet. Die 21. einkommende Verbindung wird nicht mehr angenommen.
Per Default ist die Funktion **DoS Protection** eingeschaltet.

Outgoing TLS: Eingehende Verbindungen sind immer TLS-verschlüsselt. Mit deser Funktion werden auch die ausgehenden Verbindungen automatisch stark verschlüsselt. Voraussetzung ist, dass der externe Host diese Funktion unterstützt. TLS wird auf der Firewall nur zur Verschlüsselung eingesetzt, nicht zur Authentifizierung. SMTP ist normalerweise unverschlüsselt und kann von Dritten leicht mitgelesen werden. Die Funktion sollte aus diesem Grund möglichst eingeschaltet werden.

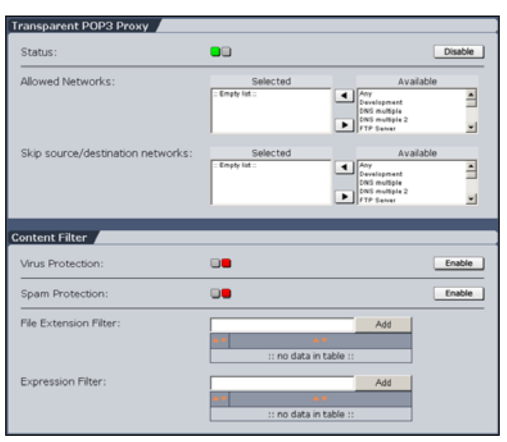
Wichtiger Hinweis:

Einige Mail-Server, z. B. Lotus Domino, haben teilweise Fehler in ihrer **TLS**-Konfiguration. Diese Mail-Server kündigen beim Verbindungsaufbau TLS an, obwohl sie durch eine unvollständige Konfiguration nicht in der Lage sind, eine TLS-Sitzung aufzubauen. Wenn TLS eingeschaltet ist, können keine E-Mails an diese Server verschickt werden. Bitte kontaktieren Sie in solch einem Fall die Administratoren dieser Mailserver.

Use Smarthost: Wenn Sie zum Versenden von E-Mails einen **Upstream Smarthost** verwenden möchten, schalten Sie diese Funktion ein und tragen den Hostnamen oder die IP-Adresse in das Eingabefeld ein. Der Proxy stellt in diesem Fall die E-Mails nicht selbst zu, sondern schickt alle an den Smarthost.

Für den Smarthost können optional noch **Benutzername** (**Username**) und **Passwort** (**Password**) definiert werden.

5.6.3. POP3



POP3 ist die Abkürzung für **Post Office Protocol 3** und ist ein Protokoll um E-Mails von einem Mail-Server zu empfangen. Das Gegenstück zu POP3 ist das Protokoll **SMTP**. SMTP steht für Simple Mail Transfer Protocol. Mit dem Protokoll werden E-Mails über einen Mail-Server versendet.

In diesem Menü konfigurieren Sie den **POP3-Proxy** für eingehende E-Mails. Der POP3-Proxy arbeitet im Transparentmodus. Die POP3-Anfragen auf Port 110 aus

dem internen Netzwerk werden abgefangen und durch den Proxy geleitet. Für den Client ist dieser Vorgang völlig unsichtbar. Es entsteht kein zusätzlicher Administrationsaufwand, da am Client des Endanwenders keine Einstellungen geändert werden müssen.

Hinweis:

Aus Sicherheitsgründen wird zum Herunterladen der E-Mails vom Mail-Server die Methode **TOP** nicht unterstützt – Nachrichten, die mit *TOP* empfangen werden, können von **POP3** nicht gescannt werden. Die Clients sollten so konfiguriert sein, dass für den Empfang von E-Mails die Methode **RETR** verwendet wird.

POP3-Proxy konfigurieren:

Beachten Sie, dass in den Drop-down-Menüs nur die Netzwerke zur Verfügung stehen, die zuvor im Menü **Definitions/Networks** definiert wurden.

1. Öffnen Sie im Verzeichnis **Proxies** das Menü **POP3**.

2. Schalten Sie den Proxy durch einen Klick auf die Schaltfläche **Enable** ein.

   Anschließend öffnet sich ein erweitertes Eingabefenster.

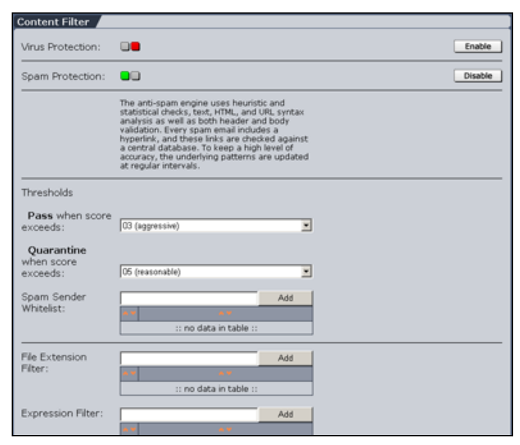
3. Wählen Sie im Auswahlfeld **Allowed Networks** die für diesen Proxy zugelassenen Netzwerke aus.

   Mit dem Auswahlfeld **Skip Source/Destination Networks** haben Sie die Möglichkeit bestimmte Netzwerksegmente oder Hosts aus den erlaubten Netzwerken auszuklammern.

   Die Funktionsweise des **Auswahlfeldes** wird in Kapitel 4.3.2 ab Seite 41 beschrieben.

Alle Einstellungen werden sofort wirksam und bleiben beim Verlassen des Menüs erhalten. Aus den zugelassenen Netzwerken kann nun auf den POP-Proxy zugegriffen werden.

5.6.3.1. Content Filter



Virus Protection: Dieses Modul untersucht E-Mails und Anhänge (Attachments) auf gefährliche Inhalte, z. B. Viren und Trojanische Pferde. Der Scanvorgang wird im E-Mail-Header vermerkt. Die gefilterten E-Mails werden im Menü **Proxies / Proxy Content Manager** angezeigt. Das Modul **Virus Protection** wird durch einen Klick auf die Schaltfläche **Enable** eingeschaltet (Statusampel zeigt Grün).

Spam Protection: Dieses Modul überprüft die eingehenden E-Mails heuristisch auf bestimmte Eigenschaften die Hinweise auf Spam geben. Hierzu dienen interne Musterdatenbanken. Auf diese Weise ist man unabhängig von den Absenderinformationen und kann somit die Genauigkeit stark erhöhen.

Wichtiger Hinweis:

Wenn Sie eine Upstream Firewall einsetzen, müssen Sie dort den Datenverkehr vom Sicherheitssystem zum Internet durch den nachfolgend aufgeführten Port erlauben. Er wird für die Kommunikation mit der **Spam-Protection**-Datenbank benötigt: UDP Port 53 (DNS).

Für den *Spam Score* können zwei **Grenzwerte** (**Thresholds**) definiert werden. Auf diese Weise können mutmaßliche SPAM E-Mails von der Firewall unterschiedlich behandelt werden.

Default-Einstellungen:

Grenzwerte (**Thresholds**)

Pass when Score exceeds: 03 (aggressive)

Quarantine when Score exceeds: 05 (reasonable)

Der erste Grenzwert hat zur Folge, dass E-Mails ab Stufe 3 gefiltert, aber durchgelassen werden. Mit Hilfe des hinzugefügten Headers kann die E-Mail auf dem Mail-Server oder im E-Mail-Programm des Empfängers sortiert oder gefiltert werden. Beim zweiten Grenzwert wird die E-Mail angenommen, kommt aber in Quarantäne.

Grundsätzliche gilt, dass der **Grenzwert** (**Threshold**) mit der höheren Stufe eine strengere Behandlung erfahren soll.

! **Wichtiger Hinweis:**

Das Modul **Spam Protection** benötigt auf stark frequentierten Systemen einen hohen Anteil der Systemressourcen.

Pass/Quarantine when Score exceeds: Mit diesen Drop-down-Menüs justieren Sie den Höchstwert zur Bewertung der E-Mails. Der Unterschied zwischen den Höchstwerten definiert sich durch die Wahrscheinlichkeit, dass ungefährliche Mails, z. B. HTML-Newsletter gefiltert werden. Im Drop-down-Menü kann ein Wert zwischen 1 und 15 eingestellt werden. Mit der Stufe 1 werden bereits E-Mails mit einem kleinen *Spam Score* behandelt. Die folgenden Stufen (Level) geben einen Anhaltspunkt:

- **Aggressive (03)**: Diese Strategie filtert die meisten Spam-Mails. Allerdings werden mit hoher Wahrscheinlichkeit auch ungefährliche Nachrichten, z. B. HTML-Newsletter zurückgewiesen.
- **Reasonable (05)**: Diese Strategie liegt zwischen **Aggessive** und **Conservative**.
- **Conservative (08)**: Diese Strategie filtert nur Nachrichten, bei denen es sich mit sehr hoher Wahrscheinlichkeit um Spam-Mails handelt. Ungefährliche E-Mails werden meist nicht gefiltert.

Die folgenden Aktionen sind voreingestellt:

- **Quarantine**: Die E-Mail wird angenommen, kommt aber in Quarantäne. Die E-Mail wird im Menü **Proxy Content Manager** mit dem Status **Quarantine** angezeigt. In diesem Menü stehen Ihnen weitere Funktionen zur Verfügung, um die E-Mail z. B. sicher zu lesen oder zu versenden.
- **Pass**: Die E-Mail wird vom Filter behandelt aber durchgelassen. Der E-Mail wird ein **Header** hinzugefügt, der es ermöglicht diese auf dem Mail-Server oder im E-Mail-Programm des Empfängers zu sortieren oder zu filtern. Des Weiteren wird in den Betreff der E-Mail der Hinweis ***SPAM*** hinzugefügt.

  Die möglichen Header sind:

  X-Spam-Score: Der Header enthält einen Punktestand, der aus einem numerischen Wert und einer Anzahl von Minus- und Pluszeichen besteht. Je höher dieser Punktestand ausfällt, umso wahrscheinlicher ist es, dass es sich bei der Nachricht um eine Spam-Mail handelt.

  X-Spam-Flag: Wenn der enthaltene Wert **Yes** lautet, wurde die Nachricht als Spam-Mail erkannt.

  X-Spam-Report: Der Proxy hat die Nachricht als Spam-Mail erkannt. Der hinzugefügte Multiline Header enthält einen offen lesbaren Antispam-Bericht.

  Wie in **Microsoft Outlook 2000** die Regeln erstellt werden wird auf Seite 325 beschrieben.

Spam Sender Whitelist: Mit dieser Kontrollliste können die E-Mails bestimmter Absender vom Scannvorgang durch das Modul **Spam Protection** ausgeschlossen werden. Es werden alle Nachrichten nicht gescannt, in denen die "*Envelope-from*"-Adresse oder "*Header*"-Absender mit einem Eintrag aus der Kontrollliste übereinstimmen.

Tragen Sie die Adressen wie nachfolgend beschrieben in die Kontrollliste ein:

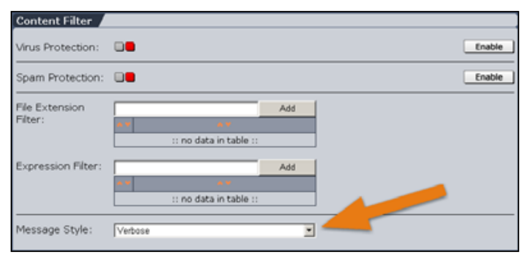
- Alle E-Mails einer bestimmten Adresse sollen nicht gescannt werden. Eingabe: user@domain.com
- Alle E-Mails einer bestimmten Domain sollen nicht gescannt werden. Eingabe: @domain.com

Die Funktionsweise der **Kontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.5 ab Seite 43 beschrieben.

File Extension Filter: Die Firewall filtert die Anhänge (Attachments) mit den Erweiterungen aus der Kontrollliste. Die verdächtige Mail wird angenommen, kommt aber in Quarantäne. Sie wird im Menü **Proxy Content Manager** mit dem Status **Quarantine** angezeigt. In diesem Menü stehen Ihnen weitere Funktionen zur Verfügung, um die E-Mail z. B. sicher zu lesen oder zu versenden.

Expressions Filter: Mit dieser Funktion können alle E-Mail-Texte und angehängte Textdateien, die durch den POP3-Proxy gehen anhand bestimmter Ausdrücke (Expressions) gefiltert werden. Verdächtige Mails werden blockiert. Die Ausdrücke werden in der Kontrollliste in Form von **Perl Compatible Regular Expressions** definiert.

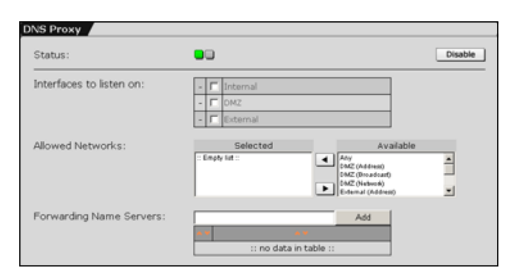
Weitere Informationen zu **Regular Expressions** finden Sie im Internet, indem Sie mit Ihrer Suchmaschine nach "Perl regular expressions tutorial" suchen.



Message Style: In diesem Drop-down-Menü können Sie einstellen, wie umfangreich die Meldung für eine in Quarantäne genommene E-Mail erstellt werden soll. Wenn alle technischen Details aufgeführt werden sollen, stellen Sie **Verbose** ein. Mit der Einstellung **Normal** werden nur die grundsätzlichen Informationen,

wie der *Absender* (*From*), der *Betreff* (*Subject*) und das *Datum* (*Date*) angezeigt.

5.6.4. DNS



Mit dem **DNS-Proxy** können Sie den Clients in Ihrem System **Nameserver**–Dienste zur Verfügung stellen. Wenn Sie mehrere angeben, werden die Server in Reihenfolge ihrer Eingabe bei der Auflösung von Rechnernamen befragt.

Die DNS-Einträge in Netzwerkdefinitionen werden jede Minute vom DNS-Resolver aufgelöst. Wenn nun ein DNS-Eintrag auf einen Round-Robin-DNS verweist, kann die Definition jede Minute aktualisiert werden. Das Round-Robin-DNS-Verfahren bietet eine einfache Möglichkeit die Benutzeranfragen auf einzelne Server, z. B. in einer Server-Farm zu verteilen. Beim Round-Robin-DNS werden im *Domain Name Service (DNS)* einem Hostnamen die IP-Adressen aller Server der Server-Farm zugeordnet. Wenn nun Clients die IP-Adresse dieses Hostnamens dort anfragen, meldet der DNS der Reihe nach diese IP-Adressen zurück. Auf diese Weise wird eine Aufteilung der Client-Anfragen auf die jeweiligen Server erreicht.
Der Nachteil beim Round-Robin-Verfahren ist, dass weder der Ausfall noch die Auslastung der einzelnen Server berücksichtigt wird.

Wenn kein Nameserver im Menü **Forwarding Name Servers** eingetragen ist, werden alle Nameserver-Anfragen an die Internet-ROOT-Nameserver geschickt. Falls Ihr Internet Service Provider oder Sie selbst einen Nameserver betreiben, sollte dieser eingetragen sein. Abfragen an diesen lokalen Nameserver sind immer schneller als Anfragen an die ROOT-Nameserver.

Die ROOT-Nameserver sind ein fester Bestandteil des Internets. 15 ROOT-Nameserver sind weltweit verteilt und bilden die Ur-Instanz für alle untergeordneten Nameserver.

Tipp:

Selbst wenn Sie den DNS-Proxy nicht benutzen möchten, ist es sinnvoll die Nameserver Ihres Internet Service Providers als Forwarder zu konfigurieren. Diese werden dann auch bei abgeschaltetem Proxy von der Firewall selbst verwendet. Damit wird zur Entlastung des ROOT-Nameservers beigetragen und die Firewall erzeugt nur lokale Anfragen, die in der Regel schneller beantwortet werden.

DNS-Proxy konfigurieren:

1. Öffnen Sie im Verzeichnis **Proxies** das Menü **DNS**.

2. Schalten Sie den Proxy durch einen Klick auf die Schaltfläche **Enable** ein.

Anschließend öffnet sich ein erweitertes Eingabefenster.

3. Führen Sie die nachfolgenden Einstellungen durch:

Interfaces to listen on: Wählen Sie die Netzwerkkarte aus, über die der DNS-Proxy erreichbar sein soll. In der Regel ist dies die interne Netzwerkkarte.
Die Netzwerkkarten werden im Menü **Network/Interfaces** konfiguriert. Die Konfiguration einer Netzwerkkarte bzw. Schnittstelle wird in Kapitel 5.3.2 ab Seite 154 beschrieben.

Die Funktionsweise der **Auswahltabelle** wird in Kapitel 4.3.3 ab Seite 42 beschrieben.

Allowed Networks: Wählen Sie die für diesen Proxy zugelassenen Netzwerke aus.



Sicherheitshinweis:

Wählen Sie im Menü **Allowed Networks** möglichst nicht **Any** aus. Der **DNS-Proxy** kann sonst von allen Internet-Teilnehmern genutzt werden.

Die Funktionsweise des **Auswahlfeldes** wird in Kapitel 4.3.2 ab Seite 41 beschrieben.

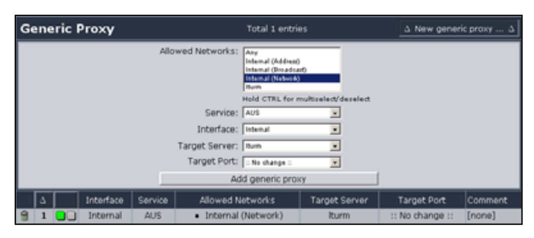
Forwarding Name Servers: Tragen Sie in das Eingabefeld die IP-Adresse des Nameservers ein.

Neue Adressen werden vom Eingabefeld durch einen Klick auf die Schaltfläche **Add** in das Hierarchiefeld übernommen.

Die Funktionsweise des **Hierarchiefeldes** wird in Kapitel 4.3.5 ab Seite 43 beschrieben.

Alle Einstellungen werden sofort wirksam und bleiben beim Verlassen des Menüs erhalten.

5.6.5. Generic



Mit dem **Generic-Proxy** können die Benutzer von Novell sicherstellen, dass der eDirectory-Verzeichnis-dienst, und auch andere Anwendungen durch das Sicherheitssystem erreichbar sind. Dabei wird auch gewährt, dass die gleiche Sicherheitsstufe besteht, wie bei dem Datenverkehr der über die protokollspezifischen Proxies weitergeleitet wird. Der Generic Proxy leitet den gesamten Datenverkehr für einen bestimmten Service zu einem frei wählbaren Server. Der Unterschied zu DNAT ist, dass dabei die Quelladresse (Source IP/Port) dieser Anfrage durch die IP-Adresse der Firewall ersetzt wird. Zusätzlich kann auch der Zielport ausgetauscht werden.

Generic-Proxy konfigurieren:

1. Öffnen Sie im Verzeichnis **Proxies** das Menü **Generic**.

2. Schalten Sie den Proxy durch einen Klick auf die Schaltfläche **Enable** ein.

   Anschließend öffnet sich ein erweitertes Eingabefenster.

3. Führen Sie die nachfolgenden Einstellungen durch:

   Die Funktionsweise der **Auswahlfelder** wird in Kapitel 4.3.2 ab Seite 41 beschrieben.

   Network: Wählen Sie das Netzwerk aus, zu dem die Weiterleitung erfolgen soll.

   Service: Wählen Sie den Dienst aus, der weitergeleitet werden soll.

   Interface: Wählen Sie die Schnittstelle für den eingehenden Datenverkehr aus.

   Target Server: Wählen Sie den Server aus zu dem der Datenverkehr weitergeleitet werden soll.

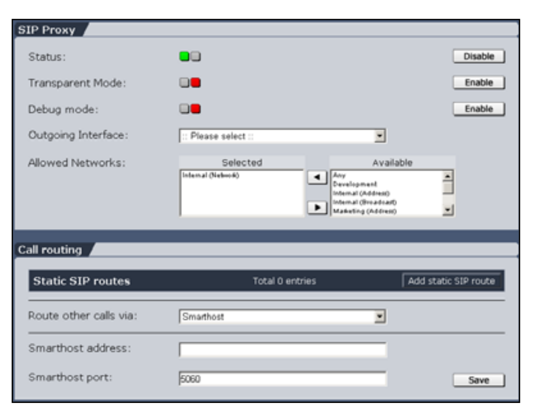
   Der Host wird im Menü **Definitions/Networks** definiert. Die Definition eines Hosts wird in Kapitel 5.2.1 ab Seite 134 beschrieben.

   Target Port: Wählen Sie den Zielport aus.

4. Fügen Sie die neue Regel durch einen Klick auf die Schaltfläche **Add generic proxy** hinzu.

Die neue Regel wird nun in die Tabelle übernommen und ist sofort aktiv. Statusampel zeigt grün.

5.6.6. SIP



Das **Session Initiation Protocol** (**SIP**) ist ein Signalisierungsprotokoll zum Aufbau, zur Modifikation und zum Beenden von Sitzungen zwischen zwei oder mehreren Kommunikationspartnern. Mit dem **SIP-Proxy** können SIP-Geräte hinter einem NAT Gateway betrieben werden. Die Sitzungsabläufe können zwar direkt zwischen den SIP-Clients ablaufen, allerdings ist nicht immer gewährleistet, dass ein Client auch erreichbar ist und immer dieselbe IP-Adresse hat. Daher meldet sich ein SIP Client in der Regel an einen SIP-Server an, der als Proxy fungiert. Der SIP-Proxy registriert die IP-Adresse. Wenn ein Anruf auf die SIP-Adresse des SIP-Clients erfolgt, wird die SIP-Adresse aufgelöst und ermittelt, wo der Client erreichbar ist. Anschließend wird der Anruf und alle anderen Anfragen an den Client weitergeleitet. Der SIP-Proxy fungiert demnach als Vermittler zwischen lokalen SIP Clients und externen SIP Providern oder Clients. Dies umfasst nicht nur die SIP-Datenfluss-Steuerung (der Standard-Port für SIP ist 5060), sondern auch das Streaming von Audiodaten. Für den Transport dieser Echtzeitdaten ist das *Real-Time Transport Protocol* (*RTP*) zuständig.

Das Modul wurde mit den folgenden SIP-Providern getestet: Free IP Call, Freenet, FWD, SimtTex, Sipgate, Stanaphone und Web.de.

SIP-Proxy definieren:

1. Öffnen Sie im Verzeichnis **Proxies** das Menü **SIP**.

2. Schalten Sie im Fenster **SIP Proxy** den Proxy durch einen Klick auf die Schaltfläche **Enable** ein.

   Anschließend öffnet sich ein erweitertes Eingabefenster.

3. Führen Sie die Grundeinstellungen durch:

   Transparent Mode: Der SIP-Proxy kann im transparenten Modus betrieben werden, um zum einen den Gebrauch des Proxy zu vereinfachen oder um auch SIP-Geräte nutzen zu können, bei denen kein Outbound-Proxy eingestellt werden kann. In diesem Modus wird der gesamte Datenverkehr an UDP Port 5060 zum Proxy geleitet.

   Debug Mode: Diese Funktion steht Ihnen zur Überprüfung der IPSec-Verbindung zur Verfügung. In den SIP-Proxy-Logs werden ausführliche Informationen protokolliert. Diese Protokolle können Sie im Menü **Local Log/Browse** in Echtzeit beobachten oder auf Ihren lokalen Rechner herunterladen. Die Funktionen im Menü **Local Logs** werden im Kapitel 5.10 ab Seite 417 beschrieben.

   Ougoing Interface: Stellen Sie in diesem Drop-Down-Menü die primäre externe Netzwerkkarte ein. Beachten Sie bitte, dass hier auch wenn das Sicherheitssystem im *Bridge Mode* betrieben wird eine IP-Adresse konfiguriert sein muss.

   Die Schnittstellen werden im Menü **Network/Interfaces** konfiguriert. Weitere Informationen zum **Bridging** erhalten Sie in Kapitel 5.2.1 auf Seite 134.

   Allowed Networks: Wählen Sie im Drop-down-Menü die Netzwerke aus, die auf diesen Proxy zugreifen dürfen. Beschrenken Sie den Zugriff auf Netzwerke innerhalb des LANs. Die Netzwerke werden im Menü **Definitions/Networks** definiert.

4. Definieren Sie im Fenster **Call Routing** wie die Weiterleitung der SIP-Anrufe durchgeführt werden soll.

4.1 Static SIP Route

Falls die SIP-Anrufe statisch weitergeleitet werden sollen, klicken Sie auf die Schaltfläche **Add static SIP route**.

Anschließend wird in die Tabelle **Static SIP Route** eine Blanko-Zeile eigefügt.
Öffnen Sie in der Spalte **SIP Domain** durch einen Klick auf die Standardeinstellung das Eingabefeld und Tragen Sie ihre Domain (z. B. freenet.de) ein. Speichern Sie die Eingabe durch einen Klick auf die Schaltfläche **Save**.

Öffnen Sie in der Spalte **Target Host:Port** durch einen Klick auf die Meldung das Eingabefeld und Tragen Sie den Ziel-Host und den Port (z. B. iphone.freenet.de:5060) ein. Speichern Sie die Eingabe durch einen Klick auf die Schaltfläche **Save**.

Die **statischen IP Routes** werden wieder aus der Tabelle entfernt, wenn Sie in der entsprechenden Zeile auf das Papierkorb-Symbol klicken.

4.2 DNS SRV / Host lookup

Diese Einstellung wird benötigt, um andere SIP Provider oder Clients zu erreichen. Standardmäßig ist diese Einstellung eingeschaltet.

4.3 Smarthost

Mit dieser Einstellung können Sie für die Weiterleitung der SIP-Anrufe einen speziellen Smarthhost definieren. Dies ist genau genommen ein SIP-Proxy, der vor das Sicherheitssystem geschaltet wird. Wenn Sie im Drop-down-Menü **Smarthost** ausgewählt haben, werden zwei weitere Eingabemenüs angezeigt.

Speichern Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

5. Führen Sie im Fenster **Advanced** die erweiterten Einstellungen durch.

   Local listening port: Standardmäßig ist hier der UDP Port 5060 eingestellt. Der **Transparent Mode** wird von dieser Einstellung nicht beeinflusst. Wenn dieser Modus eingeschaltet ist, wird daher immer nur Datenverkehr an den UDP Port 5060 zum eingestellten *Local Listening Port* umgeleitet.

   RTP port range: Jeder aktive SIP-Anruf benötigt für den Transport der Audiodaten zwei RTP Ports. Stellen Sie diesen Port-Bereich gemäß Ihren Anforderungen ein. Beachten Sie dabei, dass der lokale SIP Client von dieser Einstellung nicht beinflusst wird. Standardmäßig ist der Port-Bereich 16384:32766 eingestellt.

   RTP lifetime (seconds): Definieren Sie hier nach wieviel Sekunden ein RTP-Datenstrom als inaktiv eingestuft und abgebrochen werden soll. Standardmäßig sind 300 Sekunden eingestellt.

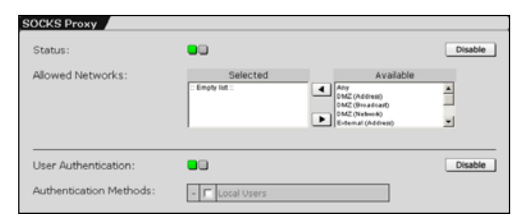
   Speichern Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

Der SIP-Proxy ist nun betriebsbereit. Führen Sie nun die Einstellungen auf den SIP-Geräten durch. Die nötigen Einstellungen entnehmen Sie bitte den zugehörigen Betriebsanleitungen.

Hinweis:

Bitte beachten Sie, dass *SIP over TCP* nicht unterstützt wird. Des Weiteren muss auf den angeschlossenen SIP-Geräten die Funktion STUN (Simple Traversal of UDP over NATs) ausgeschaltet sein. Als Alternative können Sie im Paketfilter (Packet Filter) eine Regel setzen, dass der Service STUN geblockt wird. Die Paketfilterregeln werden im Menü **Packet Filter/Rules** gesetzt.

5.6.7. SOCKS



SOCKS ist ein universeller Proxy, der von vielen Client-Applikationen unterstützt wird. Einige Beispiele dafür sind Instant Messaging Clients wie ICQ oder AIM, FTP-Clients und RealAudio. SOCKS kann stellvertretend für Clients TCP-Verbindungen aufbauen und als Besonderheit auch eingehende Verbindungen mit dem TCP- oder UDP-Protokoll annehmen (listening). Das macht SOCKS besonders auf Firewalls interessant, die NAT benutzen, da SOCKS die Nachteile von NAT ausgleichen kann. Die SOCKS-Implementation dieser Firewall unterstützt die Protokollversionen SOCKSv4 und SOCKSv5.

Bei Verwendung des SOCKSv4-Protokolls ist keine **Benutzerauthentifizierung (User Authentication)** möglich.

Hinweis:

Wenn Sie diesen Proxy verwenden möchten, um Host-Namensauflösung in SOCKS5 zu betreiben, müssen Sie auch den DNS-Proxy aktivieren.

SOCKS-Proxy konfigurieren:

1. Öffnen Sie im Verzeichnis **Proxies** das Menü **SOCKS**.
2. Schalten Sie den Proxy durch einen Klick auf die Schaltfläche **Enable** ein.

   Anschließend öffnet sich ein erweitertes Eingabefenster.
3. Führen Sie die nachfolgenden Einstellungen durch:

   Allowed Networks: Hier wählen Sie die für diesen Proxy zugelassenen Hosts und Netzwerke aus.

Die Funktionsweise des **Auswahlfeldes** wird in Kapitel 4.3.2 ab Seite 41 beschrieben.

Alle Einstellungen werden sofort wirksam und bleiben beim Verlassen des Menüs erhalten.

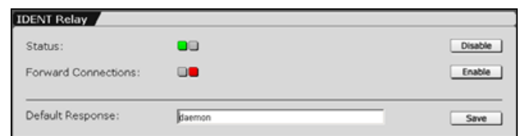
SOCKS-Proxy mit Benutzerauthentifizierung:

Wenn Sie für den SOCKS-Proxy die Funktion **User Authentication** einschalten, müssen sich die Benutzer mit Benutzernamen und Passwort anmelden. Da **User Authentication** nur mit SOCKSv5 funktioniert, ist die Protokollversion SOCKSv4 dann nicht verfügbar.

Mit dem Auswahlfeld **Authentication Methods** bestimmen Sie die Methode zur Benutzerauthentifizierung. Zur Auswahl stehen nur Authentifizierungsmethoden, die Sie zuvor im Menü **Settings/User Authentication** konfiguriert haben. Wenn Sie als Methode **Local Users** auswählen, können Sie für lokale Benutzer festlegen, ob sie den **SOCKS-Proxy** benutzen dürfen. Die lokalen **Benutzer (Users)** werden im Menü **Definitions/Users** verwaltet.

Die Funktionsweise der **Auswahltabelle** wird in Kapitel 4.3.3 ab Seite 42 beschrieben.

5.6.8. Ident



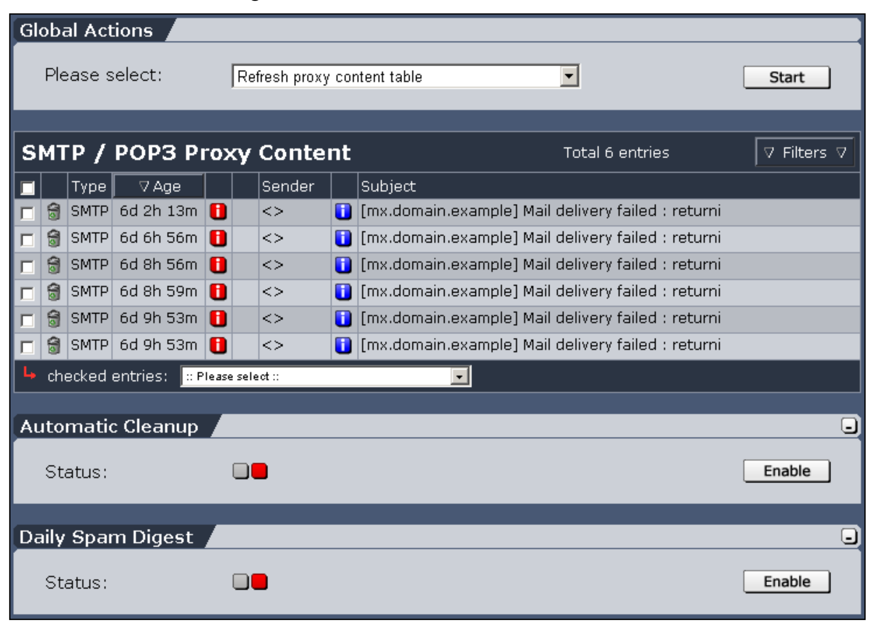
Das **Ident**-Protokoll wird von einigen Servern zur einfachen Indentitätsüberprüfung der zugreifenden Clients verwendet. Obwohl dieses Ident-Protokoll unverschlüsselt ist, verwenden es noch viele **Dienste** (**Services**) und setzen es manchmal sogar voraus.

Dieses Internet-Sicherheitssystem unterstützt zur Beantwortung Ident-Anfragen, wenn Sie die Funktion **Ident** einschalten. Das System wird immer mit dem String antworten, den Sie als **Default Response** definieren, unbeachtet dessen von welchem lokalen Dienst diese Verbindung gestartet wurde.

Forward Connections: Die Ident-Anfragen werden vom **Connection Tracking** nicht erkannt. Dies kann umgangen werden, wenn Sie die Funktion **Masquerading** verwenden. Mit **Forward Connections** können Sie die Ident-Anfragen an einen mit **Masquerading** verborgenen Host hinter die Firewall weiterleiten.
Beachten Sie dabei, dass die aktuelle IP-Verbindung nicht übergeben wird. Stattdessen wird die Firewall beim internen Client nach einer Ident-Antwort anfragen und diesen String an den externen Server weiterleiten. Dieses Vorgehen wird von den meisten Mini-Ident-Servern unterstützt, der meist Bestandteil der heute gängigen IRC- und FTP-Clients ist.

5.6.9. Proxy Content Manager

Im Menü **Proxy Content Manager** können Sie alle E-Mails einsehen, die von den Proxies der Firewall gefiltert wurden oder wegen eines Fehlers nicht weitergeleitet werden konnten.



Die nachfolgend aufgeführten Begriffe und Stati benötigen Sie, um die E-Mails in diesem Menü korrekt zu verwalten:

ID: Jede E-Mail in diesem Internet-Sicherheitssystem erhält eine eindeutige **ID**. Diese **ID** ist im Header einer Mail enthalten und identifiziert außerdem die E-Mail in den Log Files. Die **ID** wird angezeigt, wenn Sie mit der Maus den Eintrag im Feld **Type** berühren.

Type: Der Proxy Content Manager unterteilt die gefilterten E-Mails in die Typen **POP3** und **SMTP**. Wenn Sie mit der Maus den Eintrag berühren, wird die **Mail-ID** angezeigt. Durch einen Klick auf den Eintrag wird ein Fenster mit dem Inhalt der Nachricht geöffnet. Auf diese

Weise können Sie wichtige Nachrichten gefahrlos lesen. Nachrichten mit einer Länge von bis zu 500 Zeilen werden komplett dargestellt.

Age: In dieser Spalte wird das Alter der E-Mail angezeigt, d. h. der Zeitraum seit dem die Mail auf dem Internet-Sicherheitssystem eingetroffen ist.

Status: Die Stati der E-Mails im Proxy Content Manager werden durch Symbole angezeigt.

- **deferred / zurückgestellt** ( ): Die E-Mail wird an die Empfängeradresse versendet. Falls eine E-Mail mit diesem Status längere Zeit auf der Firewall liegen bleibt, so deutet dies auf temporäre Probleme auf dem Zielhost hin. Die E-Mail wird ausgeliefert, sobald der Zielhost wieder in der Lage ist, sie anzunehmen.
- **quarantined / gesperrt** (#): Die E-Mail wurde aufgrund der Einstellung **Quarantine** in einer der **Content-Filter**-Funktionen in Quarantäne genommen. In der E-Mail wurden unerwünschte oder für Ihr System sogar gefährliche Komponenten, z. B. Viren entdeckt. E-Mails mit diesem Status verbleiben in der Tabelle bis sie von Ihnen gelöscht oder explizit versendet werden.

  Bei den in Quarantäne gehaltenen E-Mails wird in der Spalte rechts neben dem Statussymbol angezeigt, durch welche Funktion die Nachricht gesperrt wurde:

  SP: Spam Protection

  VP: Virus Protection

  FILE: File Extention Filter

  EXP: Expression Filter

  MIME: MIME Error Checking
- **permanent error / andauernder Fehler** ( ): Bei dieser E-Mail besteht ein permanenter Fehler. Die Nachricht kann nicht an den Empfänger zugestellt und auch nicht an den Absender zurückgeschickt werden.

Sender: In dieser Spalte wird der Absender der E-Mail angezeigt. Beim Typ *SMTP* ist dies die Absenderadresse auf dem Umschlag.
Beim Typ *POP3* ist es die Adresse aus dem „*From:*“-Header der E-Mail. Wenn keine Absenderadresse (Envelope Sender) angezeigt wird, erhält die E-Mail den Zusatzstatus **Bounce**.

Eine *Bounce*-Nachricht ist eine Fehlermeldung, die von einem Mail-Server automatisch erstellt wird, wenn eine E-Mail nicht an den Empfänger zugestellt werden kann. Diese Fehlermeldung wird an den Absender der unzustellbaren E-Mail gesendet und hat selbst einen leeren *Envelope Sender* (Meldung: <>), um eine endlose Weiterleitung zu verhindern.

Wenn die E-Mail-Adresse eines Absenders zu lang ist, wird sie in der Spalte *Sender* gekürzt dargestellt. Falls Sie die komplette Adresse benötigen, können Sie durch einen Klick auf die *Mail-ID* in der Spalte *Type* den Inhalt der Nachricht öffnen – dort wird dann auch die ganze E-Mail-Adresse des Absenders angezeigt.

Wenn der **Content Filter** eine E-Mail blockiert hat, bei der es sich eventuell um eine **Phishing Mail** handelt, so wird dies angezeigt, wenn Sie mit der Maus die Zelle mit der Meldung **VP** berühren.
Mit diesen **Phishing Mails** locken Betrüger auf gefälschte Internetseiten und fordern Sie z. B. auf, Angaben über Passwörter und Zugangsinformationen zu Ihrem Online-Banking zu machen.

Recipient(s): In dieser Spalte wird der Empfänger der E-Mail angezeigt. Beim Typ SMTP ist dies eine Liste aller Empfängeradressen auf dem Umschlag. Bei den E-Mails mit dem Status **deferred/zurückgestellt** wird für jeden Empfänger separat der Auslieferungsstatus angezeigt: Zurückgestellt () oder andauernder Fehler ().

Im Drop-down-Menü am unteren Ende der Tabelle befinden sich mehrere Funktionen, um einzelne E-Mails zu bearbeiten. Die E-Mails müssen zuvor durch einen Klick auf das entsprechende Optionsfeld ausgewählt werden.

Folgenden Funktionen stehen zur Verfügung:

Delete: Alle ausgewählten E-Mails werden gelöscht.

Force delivery: Alle ausgewählten E-Mails werden an die Empfängeradressen weitergeleitet, auch wenn es sich um eine Nachricht mit dem Status **quarantined** handelt. Bei einer E-Mail mit dem Status **deferred** oder **permanent error** wird ein neuer Versuch gestartet die Nachricht zuzustellen. Falls durch diese E-Mail nochmals ein Fehler verursacht wird, erhält sie wieder den alten Status.

Download as .zip file: Die ausgewählten E-Mails werden in eine zip-Datei gepackt und anschließend auf dem ausgewählten lokalen Host gespeichert.

Global Actions

Um den belegten Festplattenspeicher Ihres Sicherheitssystems möglichst gering zu halten, können Sie hier alle E-Mails eines bestimmten Typs löschen. E-Mails, die während des Löschvorgangs vom Internet-Sicherheitssystem versendet oder weitergeleitet werden, sind davon nicht betroffen.
Wählen Sie im Drop-down-Menü **Please select** den Typ aus und starten Sie die Aktion durch einen Klick auf die Schaltfläche **Start**.

Wenn Sie die Tabelle **SMTP/POP3 Proxy Content** aktualisieren möchten, wählen Sie im Drop-down-Menü **Please select** die Aktion **Refresh proxy content table** aus.

Achtung:

Der ausgewählte Typ wird ohne eine nochmalige Sicherheitsabfrage gelöscht.

Filters

Mit der Funktion **Filters** können Sie aus der Tabelle *E-Mails* mit bestimmten Attributen herausfiltern. Diese Funktion erleichtert das Managen von großen Netzwerken, da Protokolle eines bestimmten Typs übersichtlich dargestellt werden können.

E-Mails filtern:

1. Klicken Sie auf die Schaltfläche **Filters**.

   Anschließend wird das Eingabefenster geöffnet.

2. Tragen Sie in den nachfolgend aufgeführten Feldern die Attribute für den Filter ein. Es müssen nicht alle Attribute definiert werden.

   Type: Falls Sie E-Mails eines bestimmten Typs filtern möchten, wählen Sie diese im Drop-down-Menü aus.

   Status: Falls Sie E-Mails mit einem bestimmten Status filtern möchten, wählen Sie diese im Drop-down-Menü aus.

   Content Filter Type: Mit diesem Drop-down-Menü filtern Sie E-Mails die mit einer bestimmten Funktion aus dem **Content Filter** gefiltert wurden.

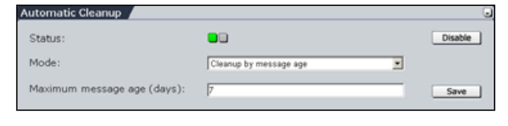
   Sender: Mit diesem Drop-down-Menü filtern Sie E-Mails mit einer bestimmten Absenderadresse.

   Recipient(s): Mit diesem Drop-down-Menü filtern Sie E-Mails mit einer bestimmten Empfängeradresse.

3. Um den Filter zu starten klicken Sie auf die Schaltfläche **Apply Filters**.

Anschließend werden nur die gefilterteten E-Mails in der Tabelle angezeigt. Nach Verlassen des Menüs werden wieder alle Protokolle dargestellt.

Automatic Cleanup



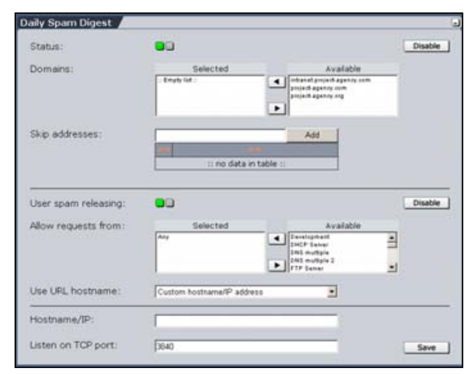
Um den belegten Festplattenspeicher Ihres Sicherheitssystems möglichst gering zu halten, können Sie hier die E-Mails automatisch löschen. Sie schalten die Funktion in der Zeile **Status** durch einen Klick auf die Schaltfläche **Enable** ein (Statusampel zeigt Grün).

Mode: Stellen Sie in diesem Drop-down-Menü den Modus ein. Folgende Modi stehen zur Auswahl:

- **Cleanup by message age**: Mit diesem Modus werden alle E-Mails ab einem bestimmten Alter gelöscht.
  Tragen Sie das Eingabefeld **Maximum Message Age (days)** das maximale Alter in Tagen ein.
- **Cleanup by message count**: Sobald sich eine bestimmte Menge an E-Mails agesammelt hat, werden die älteren E-Mails gelöscht. Per Default sind 500 E-Mails eingestellt. Weniger wie 200 sollten nicht eingestellt werden.

Die Einstellungen werden durch einen Klick auf die Schaltfläche **Save** gespreichert. Die Aktion wird anschließend einmal pro Stunde durchgeführt, so dass der maximale Stand immer nur für kurze Zeit überschritten wird.

Daily Spam Digest





Mit der Funktion **Daily Spam Digest** versendet das System eine tägliche Zusammenfassung des Proxy Content Manager an die internen Empfänger per E-Mail und informiert sie, welche eingehenden E-Mails in den letzten 24 Stunden unter Quarantäne gestellt wurden. Die E-Mail enthält eine Übersicht der gefilterten Nachrichten mit sämtlichen Informationen zu Ankunftszeit, Größe, Absender, Thema und die Meldungs-ID (für den Postmaster). Die gefilterten Nachrichten sind in umgekehrter chronologischer Reihenfolge aufgelistet, beginnend mit der Neuesten.

Sie schalten die Funktion in der Zeile **Status** durch einen Klick auf die Schaltfläche **Enable** ein (Statusampel zeigt Grün).

Domains: Wählen Sie hier die Domains aus, für die eine Übersicht erstellt werden soll. Es können nur Domains ausgewählt werden, die zuvor im Menü **Proxies/SMTP** definiert wurden.

Skip Addresses: Falls für bestimmte E-Mail-Adressen keine tägliche Spam-Übersicht erstellt werden soll, tragen Sie die entsprechende vollständige Adresse in die Kontrollliste ein.

Die Funktionsweise der **Zugriffskontrollliste** ist identisch mit dem **Hierarchiefeld** und wird in Kapitel 4.3.5 ab Seite 43 beschrieben.

User spam realising: Mit dieser Funktion haben die Benutzer durch einen Link in der **Daily Spam Digest** die Möglichkeit Informationen zu den in Quarantäne genommenen Nachrichten selbst anzufordern ohne den Administrator kontaktieren zu müssen. Falls eine zuvor in Quarantäne genommene E-Mail nicht mehr verfügbar ist, erhält der Benutzer nach der Informationsanfrage eine entsprechende Fehlermeldung.

Im Auswahlfeld **Allow Requests from** können Sie auswählen, von welchen Netzwerken oder Clients aus diese Informationen abgerufen werden können. Mit dem Drop-down-Menü **Use URL Hostname** können Sie entweder den *MX Host* verwenden, der im Menü **Proxies/ SMTP** konfiguriert ist, oder einen üblichen *Hostnamen* oder eine *IP-Adresse* angeben. Der Name oder die IP-Adresse wird im Eingabefeld **Hostname/IP** definiert. Im Eingabefeld **Listen on TCP Port** ist für die Anfragen der Port 3840 voreingestellt. Der Port kann geändert werden, falls dieser bereits für einen Anderen Dienst benötigt wird.

5.7. Virtual Private Networks (IPSec VPN)

Ein **Virtuell Private Network (VPN)** ist eine sichere Kommunikationsverbindung über ein ungesichertes Netzwerk, z. B. das Internet. Ein **VPN** ist immer dann nützlich, wenn Informationen über das Internet gesendet oder empfangen werden und gewährleistet sein muss, dass diese Informationen von keinem Dritten gelesen oder verändert werden können. Diese Verbindung wird durch die Software gesichert, die auf beiden Seiten der Verbindung installiert ist. Diese Software ermöglicht Authentifizierung, Schlüsselaustausch und Datenverschlüsselung nach dem offenen Standard **Internet Protocol Security (IPSec)**.

Bei einer durch **VPN** geschützten Verbindung können nur authentifizierte Gegenstellen miteinander kommunizieren. Niemand anderes kann Informationen über diese Verbindung übertragen, lesen oder verändern.

Eine VPN-Verbindung kann entweder zwei Hosts, einen Host und ein Netzwerk (LAN) oder zwei Netzwerke gesichert miteinander verbinden. Wenn ein VPN-Endpunkt nur aus einem Host besteht, so reicht der VPN-Tunnel bis zu diesem Rechner und wird dort ver- und entschlüsselt. Bei einem Netzwerk ist ein **Security Gateway** vorhanden, welches die VPN-Verbindung verwaltet und die Daten ver- und entschlüsselt. Der Datenverkehr zwischen dem Security Gateway und dem Netzwerk ist nicht verschlüsselt.

Der Datenaustausch zwischen zwei Gegenstellen über das **Public Wide Area Network (WAN)** erfolgt über öffentliche Router, Switches und andere Netzwerkkomponenten und wird allgemein als unsicher angesehen. Es besteht theoretisch an jedem dieser Punkte die Möglichkeit gesendete Nachrichten im Klartext mitzulesen. Mit Hilfe von **IPSec VPN** wird zwischen den beiden Endpunkten ein virtueller verschlüsselter **IP Security (IPSec)**-Tunnel durch das **WAN** erzeugt.

Ein **IPSec**-Tunnel besteht aus einem Paar richtungsgebundener **Security Associations (SA),** einem für jede Richtung der Kommunikation.

Ein **IPSec SA** besteht aus drei Komponenten:

- dem **Security Parameter Index (SPI)**,
- der IP-Adresse des Empfängers
- einem **Security Protocol** - **Authentication Header (AH)** oder **Encapsulated Security Payload (ESP)**.

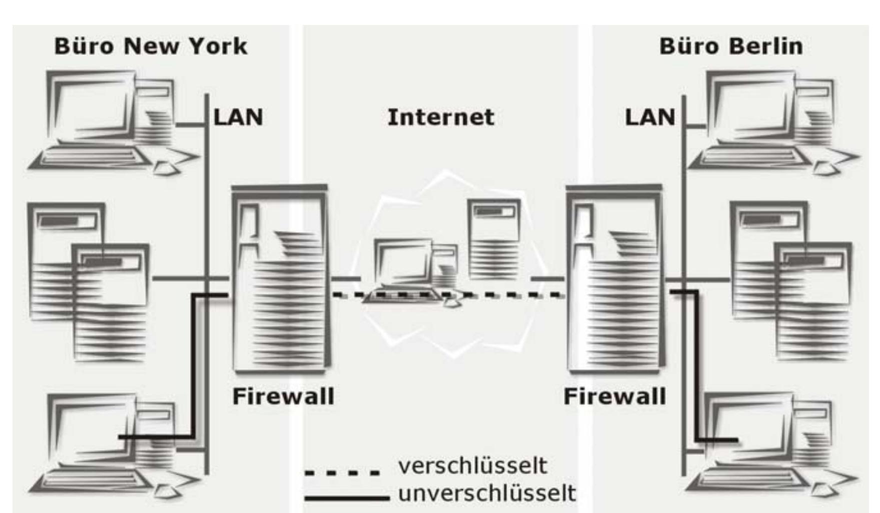
Die **SA** ermöglicht dem **IPSec VPN**-Tunnel folgende Sicherheitsfunktionen:

- Geheimhaltung durch Verschlüsselung
- Datenintegrität durch Datenauthentifizierung
- Senderauthentifizierung durch PSK, RSA oder X.509-Zertifikate

Die Sicherheitsfunktionen können beliebig kombiniert werden und richten sich nach den aktuellen Anforderungen. Die meisten Netzwerksicherheits-Designer verwenden die Verschlüsselung und die Authentifizierung.

Es gibt mehrere Szenarien IPSec VPN zu nutzen:

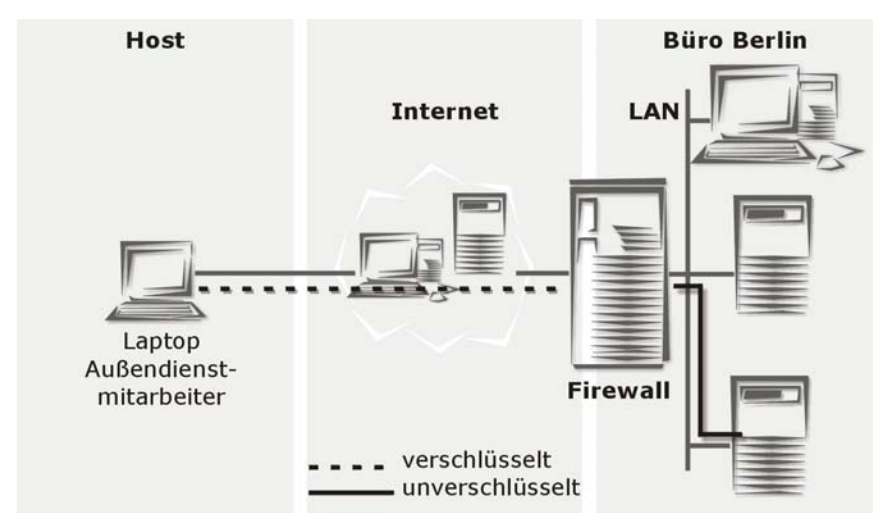
1. NET-to-NET-Verbindung



Ein Netzwerk kommuniziert mit einem anderen Netzwerk.
Zwei Unternehmens-Netzwerke von örtlich getrennten Niederlassungen können VPN nutzen, um miteinander zu kommunizieren, als wären sie ein Netzwerk.

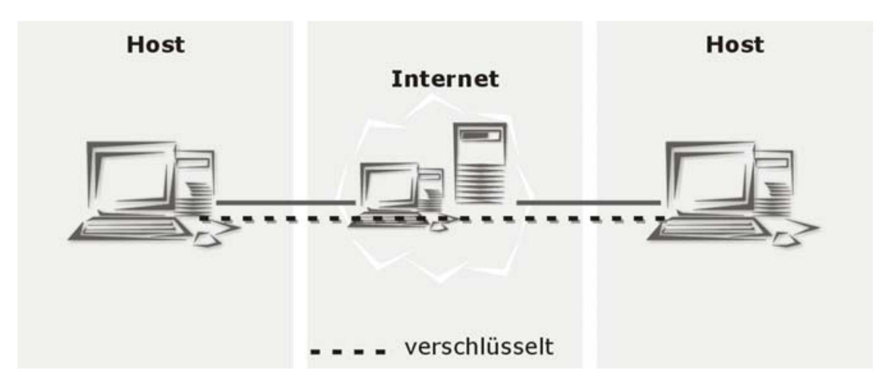
Diese Art der Verbindung könnte man auch nutzen, um vertrauenswürdigen Firmen (Zulieferer, Berater) gesicherten Zugriff auf interne Informationen zu ermöglichen.





Ein Computer kommuniziert mit einem Netzwerk.
Außendienstmitarbeiter oder Heimarbeiter können VPN benutzen, um sicher mit dem Unternehmens-Netzwerk zu kommunizieren.

3. HOST-to-HOST-Verbindung



Ein Computer kommuniziert mit einem anderen Computer.
Bei diesem Szenario können zwei Computer mittels VPN über das Internet miteinander verschlüsselt kommunizieren.

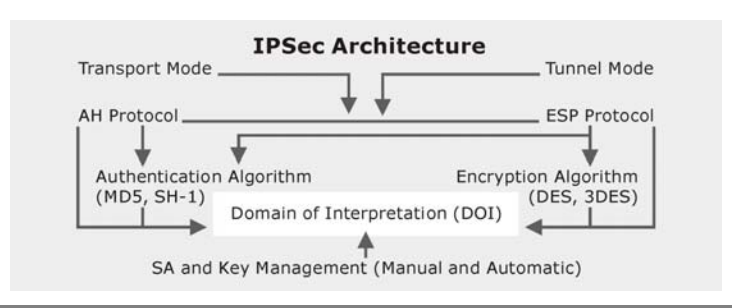
Ein VPN-Server ist eine kostengünstige und sichere Lösung um Informationen zu übertragen und kann teuere Datendirekt-Verbindungen (Standleitungen) zwischen Unternehmen ersetzen.

Das IPSec-Konzept

IP Security (IPSec) ist eine Suite von verschiedenen Protokollen für die kryptographische, sichere Kommunikation auf IP-Ebene/Layer 3 (siehe auch Kapitel 2, ab Seite 11).
IPSec besteht aus zwei Betriebsarten (Modi) und aus zwei Protokollen:

- **Transport-Modus**
- **Tunnel-Modus**
- **Authentication Header (AH)** Protokoll für Authentifizierung
- **Encapsulated Security Payload (ESP)** Protokoll für Verschlüsselung (und Authentifizierung)

Des Weiteren bietet **IPSec** Methoden für die manuelle sowie die automatische Verwaltung von **Security Associations (SA)** und zur Schlüsselverteilung. Alle diese Merkmale wurden in einem **Domain of Interpretation (DOI)** zusammengefasst.

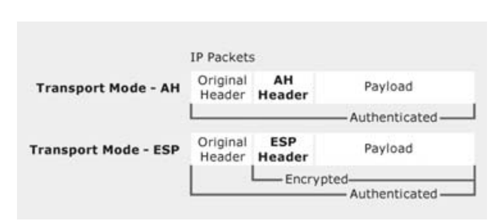


Hinweis:

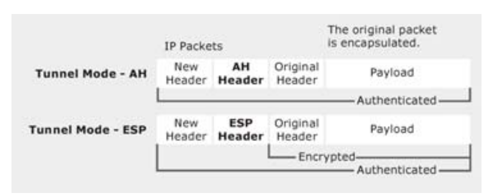
Das Internet-Sicherheitssystem unterstützt den **Tunnel Mode** und das **Encapsulated Security Payload (ESP)** Protokoll.

IPSec Modi

IPSec arbeitet im **Transport-Modus** oder **Tunnel-Modus**. Bei einer Host to Host-Verbindung kann grundsätzlich entweder Transport oder Tunnel Modus verwendet werden. Falls einer der beiden Tunnelend-punkte ein Security Gateway ist, muss der Tunnel Modus verwendet werden. Die IPSec VPN-Verbindungen dieses Internet-Sicherheits-systems arbeiten immer im Tunnel-Modus.



Beim **Transport-Modus** wird das zu bearbeitende IP-Paket nicht in ein anderes IP-Paket eingepackt. Der ursprüngliche IP-Header wird beibehalten und das übrige Paket wird nach einem entsprechenden Protokoll Header als Payload entweder im Klartext **(AH)** oder verschlüsselt **(ESP)** angehängt. Nun kann entweder das komplette Paket mit **AH** authentifiziert oder die Payload mit Hilfe von **ESP** verschlüsselt und authentifiziert werden.
Bei beiden Varianten wird der original Header in Klartext über das WAN geschickt.



Beim **Tunnel-Modus** wird das komplette Paket – Header und Payload – in ein neues IP-Paket als Payload eingepackt. Ein neuer IP-Header wird vorne an das IP-Paket angehängt. Die IP-Adressen des neuen Header entsprechen denen der IPSec-Tunnelendpunkte. Die IP-Adressen des eingepackten Paketes bleiben unverändert. Das komplette Originalpaket kann nun mit **AH** authentifiziert oder mit **ESP** authentifiziert und verschlüsselt werden.

IPSec-Protokolle

IPSec verwendet für die sichere Kommunikation auf der IP-Ebene zwei Protokolle.

- **Authentication Header (AH)** – ein Sicherheitsprotokoll für die Authentifizierung des Absenders sowie zur Überprüfung der Integrität des Inhalts
- **Encapsulating Security Payload (ESP)** – ein Sicherheitsprotokoll für die Verschlüsselung des kompletten Paketes (sowie für die Authentifizierung des Inhalts)

Das **Authentication Header**-Protokoll **(AH)** ermöglicht die Überprüfung der Authentizität und der Integrität des Paketinhalts. Des Weiteren wird geprüft, ob die Sender- und Empfänger-IP-Adresse geändert wurde. Die Authentifizierung des Pakets erfolgt anhand einer Prüfsumme, die mittels eines Hash-based Message Authentication Codes (HMAC) in Verbindung mit einem Schlüssel und einem der folgenden Hash-Algorithmen berechnet wurde:

Der **Message Digest Version 5 (MD5)-**Algorithmus erzeugt aus einer Nachricht mit beliebiger Länge einen 128 bit langen Hash-Wert. Dieser resultierende Hash-Wert wird als eine Art Fingerabdruck des Paketinhalts verwendet, um den Absender zu prüfen. Dieser Hash-Wert wird auch als **digitale Signatur** oder als **Message Digest** bezeichnet.

Der **Secure Hash (SHA-1)**-Algorithmus erzeugt analog zum **MD5** einen 160 bit langen Hash-Wert. **SHA-1** ist aufgrund des längeren Schlüssels sicherer als **MD5**.

Der Aufwand einen Hash-Wert mittels **SHA-1** zu berechnen ist im Vergleich zum **MD5**-Algorithmus etwas höher. Dies kommt allerdings infolge der heutigen Prozessor-Performance nur zum tragen, wenn sehr viele **IPSec VPN**-Verbindungen über ein **Security Gateway** verschlüsselt werden.

Das **Encapsulated Security Payload**-Protokoll **(ESP)** bietet zusätzlich zur Verschlüsselung auch die Möglichkeit der Absender –Authentifizierung und der Inhaltsverifizierung. Wenn man **ESP** im **Tunnel-Modus** verwendet, wird das komplette IP-Paket (Header und Payload) verschlüsselt. Zu diesem verschlüsselten Paket wird ein neuer unverschlüsselter IP- und ESP-Header hinzugefügt. Der neue IP-Header beinhaltet Absender- und Empfänger-IP-Adresse. Diese IP-Adressen entsprechen denen des VPN-Tunnels.

Für **ESP** mit Verschlüsselung werden üblicherweise die folgenden Verschlüsselungs verwendet:

- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)

Eine hohe Sicherheit erreicht man durch Verwenden von AES. Die effektiven Schlüssellängen von AES sind wahlweise 128, 192 oder 256 Bits. Die IPSec VPN-Funktion dieses Internet-Sicherheitssystems unterstützt mehrere Verschlüsselungs-Algorithmen.

Für die Authentifizierung kann wieder der MD5- oder der SHA-1-Algorithmus verwendet werden.

Schlüsselverwaltung (Key Management)

Die sichere Erzeugung, Verwaltung und Verteilung der Schlüssel ist ausschlaggebend für die erfolgreiche Nutzung einer VPN-Verbindung. IPSec unterstützt die manuelle (Manual Keying) sowie die automatische Schlüsselverteilung (Internet Key Exchange).

Für die **manuelle Schlüsselverteilung (Manual Keying)** müssen beide Seiten des VPN-Tunnels von Hand konfiguriert werden. Im Detail bedeutet dies, dass für jede der beiden **Security Associations (SA)** – immer zwei je VPN-Tunnel – ein **Security Parameter Index (SPI)** ausgewählt, je ein Schlüssel für die Verschlüsselung und die Authentifizierung generiert werden muss und diese Schlüssel auf beiden Seiten installiert werden müssen. Diese Schlüssel sollten später in regelmäßigen Abständen gegen neue ersetzt werden.

Die manuelle Schlüsselverteilung ist sehr aufwendig. Des Weiteren birgt dieses Verfahren einige Sicherheitsrisiken, da gewährleistet sein muss, dass Unbefugte keinen Zugang zu den Schlüsseln haben.
Bei neuen Installationen wird **Manual Keying** heute nur noch selten verwendet.

Mit Hilfe des **Internet Key Exchange (IKE)**-Protokolls führt **IPSec** die Schlüsselverwaltung selbständig durch. Die Schlüssel werden automatisch erzeugt und sicher ausgetauscht. Das **IKE**-Protokoll ermöglicht das Erzeugen und Verwalten mehrerer VPN-Tunnel sowie die Verwendung von dynamischen IP-Adressen. Außerdem werden vom **IKE**-Protokoll die **Security Associations (SA)** automatisch verwaltet.

Das Internet-Sicherheitssystem unterstützt drei Authentifizierungsarten innerhalb des IKE-Protokolls:

- IKE mit Preshared Keys (PSK)
- IKE mit RSA Keys (RSA)
- IKE mit X.509v3-Zertifikaten (X.509)

Die Authentifizierung mit **Preshared Keys (PSK)** erfolgt durch Schlüssel mit einem geheimen Kennwort, die vor der eigentlichen Verbindung unter den Beteiligten ausgetauscht werden. Wenn nun ein VPN-Tunnel aufgebaut werden soll, prüfen die beiden Gegenstellen, ob ihnen dieses geheime Kennwort bekannt ist. Wie sicher solche **PSK**s sind, hängt davon ab, wie „gut“ das Kennwort gesetzt wurde. Allgemeine Wörter sind z. B. sehr unsicher, da sie sehr anfällig auf Wörterbuch-Angriffe sind. Daher sollte bei dauerhaften IPSec VPN-Verbindungen diese Authentifizierungsmethode durch Zertifikate oder durch RSA ersetzt werden.

Die Authentifizierung mit **RSA Keys** basiert auf einem Schlüssel-(Key)-Paar und beinhaltet einen **Public Key** (öffentlichen Schlüssel) und einen **Private Key** (privaten Schlüssel). Der **Private Key** wird zur Verschlüsselung und Authentifizierung während des **Key Exchanges** (Schlüsselaustausch) benötigt. Die beiden Schlüssel sind

mathematisch voneinander abhängig und stehen in einer einzigartigen Verbindung zueinander: Daten, die mit einem Schlüssel verschlüsselt wurden, können nur mit dem anderen Schlüssel wieder entschlüsselt werden. Der **Private Key** kann nicht mit vertretbarem Aufwand vom **Public Key** abgeleitet werden.

Beide Gegenstellen einer IPSec VPN-Verbindung benötigen bei dieser Authentifizierungsmethode ihren eigenen **Public Key** und **Private Key**.

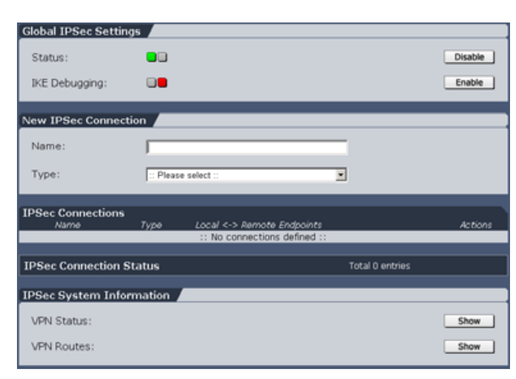
Das **X.509-Zertifikat** basiert ähnlich wie die Authentifizierung mit RSA Keys auf den Schlüsselpaaren **Public Key** und **Private Key**. Ein X.509-Zertifikat entspricht dem **Public Key** mit zusätzlichen spezifischen Informationen. Dieses Zertifikat wird wird durch eine **Certificate Authority (CA)** Ihres Vetrauens signiert. Während des **Key Exchange** werden die Zertifikate ausgetauscht und durch das lokal gespeicherten CA-Zertifikat überprüft.

Weitere Informationen zu **Certificate Authority (CA)** erhalten Sie in Kapitel 5.1.10 ab Seite 119 und in Kapitel 5.7.6 ab Seite 389.

5.7.1. Connections

Im Menü **Connections** definieren Sie die lokalen Einstellungen für einen neuen **IPSec**-Tunnel oder editieren und beobachten die bestehenden Verbindungen.

Global IPSec Settings



In diesem Fenster schalten Sie **IPSec VPN** durch einen Klick auf die Schaltfläche **Enable/Disable** neben **Status** ein und aus.

IKE Debugging: Diese Funktion steht Ihnen zur Überprüfung der IPSec-Verbindung zur Verfügung. In den IPSec-Logs werden ausführliche Informationen protokolliert. Diese Protokolle können Sie im Menü **Local Log/Browse** in Echtzeit beobachten oder auf Ihren lokalen Rechner herunterladen. Die Funktionen im Menü **Local Logs** werden im Kapitel 5.10 ab Seite 417 beschrieben.

Wichtiger Hinweis:

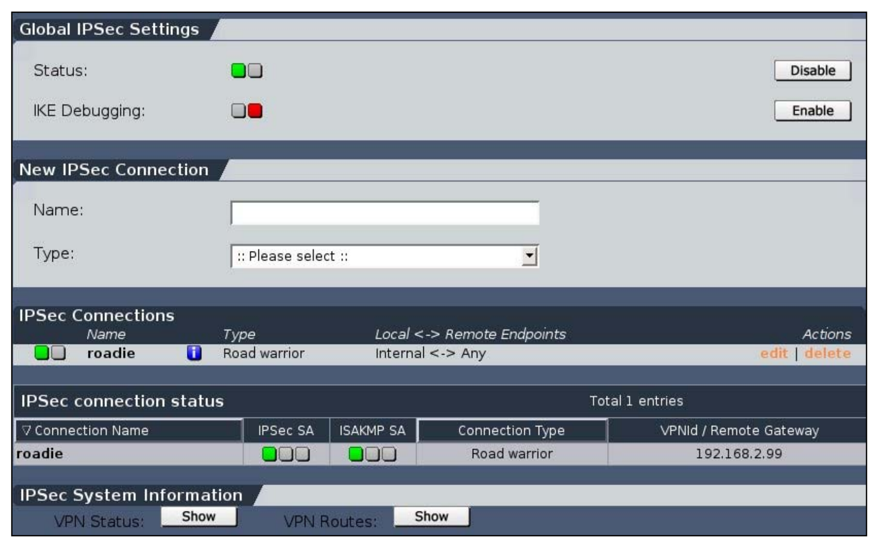
Die Funktion **IKE Debugging** benötigt einen großen Teil der Systemresourcen und kann daher den IPSec VPN-Verbindungsaufbau erheblich verlangsamen. Schalten Sie daher die Funktion nur für den eigentlichen Debugging-Vorgang ein.

IPSec Connections

In der Tabelle **IPSec Connections** werden alle aktuellen IPSec-VPN-Verbindungen angezeigt.

IPSec Connection Status

In der Tabelle **IPSec Connection Status** werden alle aktuell ausgehandelten oder aufgebauten IPSec-VPN-Verbindungen angezeigt.



Eine Verbindung ist vollständig aufgebaut, wenn die Statusampeln in den Spalten **IPSec SA** und **ISAKMP SA** beide grün anzeigen. Die Tabelle enthält die folgenden Meldungen:

Connection Name: Der Name für die IPSec-VPN-Verbindung.

IPSec SA: Meldet den Status der IPSec SA: rot = inaktiv, gelb = wird ausgehandelt, grün = aufgebaut.

ISAKMP SA: Meldet den Status der ISAKMP SA: rot = inaktiv, gelb = wird ausgehandelt, grün = aufgebaut.

Connection Type: Der im Konfigurationstool **WebAdmin** eingestellte Verbindungs-Typ.

VPNid / Remote Gateway: Die entfernte *VPN ID* (wenn keine IP-Adresse) und die aktuelle IP-Adresse der Gegenstelle.

IPSec System Information



VPN Status: Im Fenster **VPN Status** wird der Status der aktiven Verschlüsselungs-Algorithmen, alle aktiven IPSec-Verbindungen und detaillierte Informationen zu jeder **Security Association (SA)** angezeigt.

VPN Routes: Im Fenster **VPN Routes** werden alle aktiven IPSec-SA-Verbindungen angezeigt. Solange hier keine Einträge vorhanden sind, existieren keine IPSec-Verbindungen.

Routing-Einträge werden nach folgendem Schema angezeigt:

```
A B                 -> C                => D
3 192.168.105.0/24 -> 192.168.104.0/24 => %hold
8 192.168.105.0/24 -> 192.168.110.0/24 => %trap
0 192.168.105.0/24 -> 192.168.130.0/24 =>
                      tun0x133a@233.23.43.1
```

Spalte **A**: Anzahl der Pakete in dieser VPN-Verbindung.

Spalte **B**: Das lokale Sub-Netzwerk oder den Host.

Spalte **C**: Das entfernte Sub-Netzwerk oder den Host.

Spalte **D**: Der Status der VPN-Verbindung.

%trap: Die Verbindung ist im Leerlauf und wartet bis ein Datenpaket eintrifft. Dieser Status leitet die Aushandlung der VPN-Verbindung ein.

%hold: Die Aushandlung dauert an. Das bedeutet, dass alle Datenpakete gehalten werden bis der VPN-Tunnel hochgefahren (UP) ist.

tun0x133a@233.23.43.1: Diese oder eine ähnliche Meldung wird angezeigt, sobald der Tunnel hochgefahren ist:

Ein VPN-Tunnel mit der ID 0x133a ist hochgefahren und die IP-Adresse des **Remote Endpoint** ist 233.23.43.1.

Beispiel:

```
A B                  -> C                  => D

23 192.168.105.0/24 -> 192.168.104.0/24 =>
                       tun0x1234@123.4.5.6
```

In diesem VPN-Tunnel wurden 23 Datenpakete vom Netzwerk 192.168.105.0/24 zum Netzwerk 192.168.104.0/24 geschickt. Der Tunnel hat die ID 0x1234 und der Remote Endpunkt hat die IP-Adresse 123.4.5.6..

IPSec-Verbindung konfigurieren:

1. Öffnen Sie im Verzeichnis **IPSec VPN** das Menü **Connections**.
2. Schalten Sie im Fenster **Global IPSec Settings** das Modul durch einen Klick auf die Schaltfläche **Enable** ein.

   Anschließend wird das Fenster **New IPSec Connection** geöffnet.
3. Führen Sie die folgenden Grundeinstellungen für die IPSec-VPN-Verbindung durch:

   Name: Definieren Sie einen Namen, der diesen IPSec-VPN-Tunnel eindeutig beschreibt. Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9 und Unterstrich.

   Type: Wählen Sie hier den Verbindungs-Typ aus.

   Der Typ **Standard** dient für **NET to NET**-Verbindungen.

   Die Typen **Road Warrior**, **Road Warrior CA** und **MS Windows L2TP over IPSec** eignen sich für **HOST-to-NET**-Verbindungen, wie z. B. für Außendienstmitarbeiter. Diese können über ihr Laptop eine IPSec-Verbindung zum firmeninternen LAN aufbauen. Eine Road-Warrior-Verbindung kann nur über ein **Default Gateway** angeschlossen werden.

Wichtiger Hinweis:

An eine Road-Warrior-Verbindung können mehrere Remote-Key-Objekte hinzugefügt werden. Der Konfigurationsaufwand wird dadurch erheblich verringert. Allerdings ist darauf zu achten, dass bei allen Road Warriors die gleiche Authentifizierungsart (PSK, RSA oder X.509) verwendet wird - ein Mischbetrieb kann zu Funktionsstörungen führen.

Die weiteren Einstellungen richten sich nach dem ausgewählten Verbindungs-Typ.

4. Führen Sie die spezifischen Einstellungen für den Verbindung-Typ durch.

IPSec Policy: In der Policy werden die Parameter für die IPSec-Verbindung generiert. Dies beinhaltet die Einstellung der **Key Exchange-**Methode **IKE** und der **IPSec**-Verbindung.

Im Drop-down-Menü sind bereits vordefinierte Policies enthalten. Im Menü **IPSec VPN/Policies** können Sie eigene **IPSec Policies** konfigurieren.

Hinweis:

Für den Verbindungs-Typ **MS Windows L2TP IPSec** wird eine Standard-Policy verwendet.

Die Konfiguration einer **IPSec Policy** wird in Kapitel 5.7.2 ab Seite 374 beschrieben.

Auto Packet Filter: Sobald die IPSec-VPN-Verbindung aufgebaut wurde, werden die Paketfilterregln für den Datenverkehr automatisch hinzugefügt. Beim Beenden der Verbindung, werden die Paketfilterregeln wieder entfernt.

Die Funktion **Auto Packet Filter** ist für die Verbindungs-Typen **Standard** und **Road Warrior** verfügbar.



Sicherheitshinweis:

Wenn Sie die Security Policy konsequent durchführen möchten, schalten Sie die Funktion **Auto Packet Filter** aus und setzen stattdessen die entsprechende Paketfilterregel im Menü **Packet Filter / Rules**.

Strict Routing: Wenn die Funktion eingeschaltet ist (**On**), erfolgt das VPN-Routing nicht nur mit der Zieladresse, sondern in Übereinstimmung mit der Quell- und der Zieladresse.
Bei eingeschaltetem *Strict Routing* ist es möglich von verschiedenen Quelladressen zu einem Netzwerk gleichzeitig unverschlüsselte und verschlüsselte Verbindungen einzustellen.

Wenn die Funktion **Strict Routing** ausgeschaltet ist (**Off**), können durch Setzen von **Source NAT**-Regeln weitere Netzwerke und Hosts an den IPSec-VPN-Tunnel angeschlossen werden.

Die Funktion **Strict Routing** kann nur beim Verbindungs-Typ **Standard** ein- und ausgeschaltet werden. Bei allen anderen Verbindungs-Typen ist die Funktion immer eingeschaltet!

5. Wählen Sie im Fenster **Endpoint Definition** die Endpunkte des IPSec-Tunnels aus.

   Local Endpoint: Wählen Sie im Drop-down-Menü den lokalen Endpunkt aus. Wählen Sie hierfür immer die Netzwerkkarte aus, die in Richtung des anderen Endpunktes zeigt.

   Remote Endpoint: Wählen Sie im Drop-down-Menü den entfernten Endpunkt aus.
   Bei den Verbindungs-Typen *Road Warrior* oder *MS Windows L2TP over IPSec* hat der entfernte Endpunkt immer eine dynamische IP-Adresse.

6. Im Fenster **Subnet Definition (optional)** können Sie für beide Endpunkte optional ein Sub-Netzwerk auswählen.

   Local Subnet: Wählen Sie hier das lokale Sub-Netzwerk aus.

Remote Subnet: Wählen Sie hier das entfernte Sub-Netzwerk aus.

Bei einer **Road-Warrior**-Verbindung, kann nur das lokale Sub-Netzwerk eingestellt werden. Diese Möglichkeit entfällt, wenn Sie für die *Road-Warrior*-Verbindung in Schritt 7 die Funktion **L2TP Encapsulation** einschalten.

Virtual IP Address Pool: Diese Funktion wird nur angezeigt, wenn Sie in Schritt 3 den Verbindungs-Typ **Road Warrior CA** eingestellt haben. Der Road Warrior kann sich dann nur einwählen, wenn die virtuelle IP-Adresse aus dem Adress-Bereich stammt.

Hinweis:

Beim Verbindungs-Typ **MS Windows L2TP IPSec** wird das Fenster nicht angezeigt. Der IPSec-VPN-Zugang wird durch den **Paketfilter** (**Packet Filter**) geregelt.

---

7. Wählen Sie nun im Fenster **Authentication of Remote Station(s)** den passenden **Key** aus.
   Die IPSec-Remote-Keys werden im Menü **IPSec VPN/Remote Key** definiert. Die Einstellungen in diesem Fenster hängen vom Verbindungs-Typ ab.

7. 1 Standard

Key: Wählen Sie im Drop-down-Menü den **Remote Key** aus.

7.2 Road Warrior

L2TP Encapsulation: In diesem Drop-down-Menü können Sie zuätzlich **L2TP over IPSec** einschalten (**On**).

Keys: Wählen Sie im Auswahlfeld die **Remote Keys** für die Road-Warrior-Verbindungen aus.

7.3 Road Warrior CA

L2TP Encapsulation: In diesem Drop-down-Menü können Sie zusätzlich **L2TP over IPSec** einschalten (**On**).

Use CA: Beim Verbindungs-Typ *Road Warrior CA* basiert die Authentifizierung auf dem **Distinguished Name** (**DN**) der entfernten Gegenstelle (**Remote Endpoint**). Daher benötigen Sie von dieser Gegenstelle ein **Certificate Authority (CA)**. Es kann nur der VPN Identifier **X.509 DN** verwendet werden.

Wählen Sie im Drop-down-Menü das **X.509 DN Certificate Authority (CA)** aus.

Client DN Mask: Für den VPN-ID-Type **Distinguished Name** benötigen Sie die folgenden Daten aus dem X.509-Verzeichnisbaum: Country (C), State (ST), Local (L), Organization (O), Unit (OU), Common Name (CN) und E-Mail Address (E).
Die Daten müssen in diesem Eingabefeld in der gleichen Reihenfolge wie im Zertifikat aufgeführt sein.

7.3 MS Windows L2TP IPSec

L2TP Encapsulation: Bei diesem Verbindungs-Typ ist **L2TP over IPSec** automatisch eingeschaltet (**On**).

IPSec Shared Secret: Beim Verbindungs-Typ *MS Windows L2TP IPSec* basiert die Authentifizierung auf **Preshared Keys**.
Tragen Sie in das Eingabefeld das Kennwort ein.

8. Speichern Sie nun die Einstellungen durch einen Klick auf die Schaltfläche **Add**.

Das neu konfigurierte IPSec-Verbindungsprofil wird immer deaktiviert an letzter Stelle in die Tabelle eingetragen (Statusampel zeigt Rot). Durch einen Klick auf die Statusampel wird die IPSec-Verbindung aktiviert.

Nachdem Sie einen VPN-Tunnel erstellt haben, müssen Sie noch die entsprechenden Paketfilterregeln setzen, die es den jeweiligen Partei-

en erlauben, miteinander zu kommunizieren.
Das Setzen von Paketfilterregeln wird in Kapitel 5.4 ab Seite 223 beschrieben.

Beispiel:

Wenn Sie eine Net-to-Net-VPN-Verbindung (zwischen Netzwerk 1 und Netzwerk 2) erstellt haben und die komplette Kommunikation zwischen diesen beiden Netzwerken erlauben möchten, müssen Sie die folgenden zwei Regeln setzen:

1. Öffnen Sie im Verzeichnis **Packet Filter** das Menü **Rules**.
2. Setzen Sie im Fenster **Add Rules** die folgende Regel für das Netzwerk 1:

   Source: Netzwerk1

   Service: Any

   Destination: Netzwerk2

   Action: Allow
3. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add Definition**.
4. Setzen Sie im Fenster **Add Rules** die folgende Regel für das Netzwerk 2:

   Source: Netzwerk2

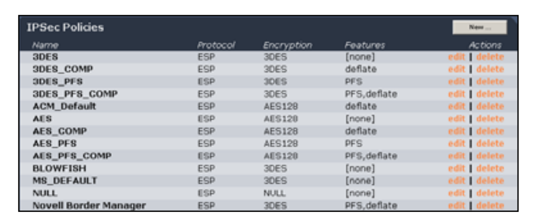
   Service: Any

   Destination: Netzwerk1

   Action: Allow
5. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Add Definition**.

Anschließend ist die komplette Kommunikation zwischen den beiden VPN-Gegenstellen möglich.

5.7.2. Policies



IPSec Policies

Name	Protocol	Encryption	Features	Actions
3DES	ESP	3DES	[none]	edit | delete
3DES_COMP	ESP	3DES	deflate	edit | delete
3DES_PFS	ESP	3DES	PFS	edit | delete
3DES_PFS_COMP	ESP	3DES	PFS,deflate	edit | delete
ACM_Default	ESP	AES128	deflate	edit | delete
AES	ESP	AES128	[none]	edit | delete
AES_COMP	ESP	AES128	deflate	edit | delete
AES_PFS	ESP	AES128	PFS	edit | delete
AES_PFS_COMP	ESP	AES128	PFS,deflate	edit | delete
BLOWFISH	ESP	3DES	[none]	edit | delete
MS_DEFAULT	ESP	3DES	[none]	edit | delete
NULL	ESP	NULL	[none]	edit | delete
Novell Border Manager	ESP	3DES	PFS,deflate	edit | delete

Im Menü **Policies** definieren Sie die Parameter für die IPSec-Verbindung und generieren daraus eine Policy. Die Policy wird für die Erstellung einer IPSec-Verbindung benötigt und beinhaltet die Konfiguration der **Key Exchange**-Methode **IKE** und die der **IPSec**-Verbindung.

Der **Key Exchange** steht für die Art des Schlüsselaustausches der IPSec-Verbindung.

Die gängigen Varianten sind:

- Manual Key Exchange
- Internet Key Exchange (IKE)

Das IPSec VPN dieses Internet-Sicherheitssystems unterstützt IKE als Key-Exchange-Methode. Die Manual-Key-Exchange-Methode ist nicht möglich.

IPSec Policy konfigurieren:

1. Öffnen Sie im Verzeichnis **IPSec VPN** das Menü **Policies**.

2. Klicken Sie auf die Schaltfläche **New** um das Menü **New IPSec Policy** zu öffnen.

3. Tragen Sie im Eingabefeld **Name** einen Namen für die neue IPSec Policy ein:

Name: Definieren Sie einen Namen, der diese Policy eindeutig beschreibt, z. B. den verwendeten Verschlüsselungs-Algorithmus. Sie können den Namen auch im letzten Schritt vor dem Erzeugen der Policy definieren.

Key Exchange: Als Schlüsselaustauschs-Methode wird nur **IKE** unterstützt.

4. Definieren Sie im Fenster **ISAKMP (IKE) Settings** die Einstellungen für die IKE-Verbindung:

   IKE Mode: Der IKE-Modus beschreibt das für den Schlüsselaustausch nötige Protokoll. Derzeit wird nur **Main Mode** unterstützt.

   Encryption Algorithm: Der Encryption Algorithmus beschreibt den Algorithmus für die Verschlüsselung der IKE-Verbindung. Die IPSec VPN-Funktion dieses Internet-Sicherheitssystems unterstützt **1DES 56bit**, **3DES 168bit**, **AES (Rijndael) 128bit**, **AES Rijndael 192bit**, **AES Rijndael 256bit**, **Blowfish**, **Serpent 128bit** und **Twofish**.

   Authentication Algorithm: Hier wird angezeigt, welcher Algorithmus verwendet wird, um die Vollständigkeit der IKE-Nachricht zu prüfen. Unterstützt werden die Algorithmen **MD5 128 bit**, **SHA1 160bit**, **SHA2 256bit** und **SHA2 512bit**. Der zu verwendende Algorithmus wird von der Gegenstelle der IPSec-Verbindung bestimmt.

   Wichtiger Hinweis:

   Die Algorithmen **SHA2 256bit** und **SHA2 512bit** benötigen einen hohen Anteil der Systemresourcen.

   IKE DH Group: Die IKE Group (Diffie-Hellmann Group) bezeichnet und beschreibt die asymetrische Verschlüsselung während des Schlüsselaustauschs. Die IPSec VPN-Funktion dieses Internet-Sicherheitssystems unterstützt **Group 1 (MODP768)**, **Group 2 (MODP 1024)**, **Group 5 (MODP 1536)**, **Group X (MODP 2048)**, **Group X (MODP 3072)** und **Group X (MODP 4096)**. Die zu verwendende Gruppe wird von der Gegenstelle der IPSec-Verbindung bestimmt.

   SA Lifetime (secs): Hier definieren Sie die Dauer der IKE-Verbindung in Sekunden. Nach der Installation sind standardmäßig 7800 Sekunden (2h, 10 min) eingestellt.

Generell ist eine Zeitspanne zwischen 60 und 28800 Sekunden (8 Stunden) möglich.

5. Definieren Sie im Fenster **IPSec Settings** die Einstellungen für die IPSec-Verbindung:

   IPSec Mode: Dieses System unterstützt den **Tunnel Mode**.

   IPSec Protocol: Dieses System unterstützt nur das Protokoll **ESP**.

   Encryption Algorithm: Hier wählen Sie den Algorithmus für die Verschlüsselung der IPSec-Verbindung aus.
   Dieses System unterstützt die Verschlüsselungs-Algorithmen **1DES 56bit**, **3DES 168bit**, **AES (Rijndael) 128bit**, **AES Rijndael 192bit**, **AES Rijndael 256bit**, **Blowfish**, **Serpent 128bit** und **Twofish**. Wenn Sie die IPSec-Verbindung ohne Verschlüsselung aufbauen möchten wählen Sie **null** aus.

   Enforce Algorithm: Wenn ein IPSec Gateway einen Vorschlag bzgl. eines Verschlüsselungsalgorithmus und der Stärke macht, kann es vorkommen, dass das Gateway der Gegenstelle diesen Vorschlag annimmt, obwohl die IPSec Policy diesem nicht entspricht. Um dies zu verhindern, muss **Enforce Algorithm** aktiviert werden.

   Beispiel:

   Die IPSec Policy fordert AES-256 als Verschlüsselung. Ein Road Warrior mit **SSH Sentinel** will aber mit AES-128 verbinden. Ohne **Enforce Algorithm** wird die Verbindung trotzdem zugelassen, was ein Sicherheitsrisiko darstellt.

   Authentication Algorithm: Unterstützt werden die Algorithmen **MD5 128bit**, **SHA1 160bit**, **SHA2 256bit** und **SHA2 512bit**. Der zu verwendende Algorithmus wird von der Gegenstelle der IPSec-Verbindung bestimmt.

Wichtiger Hinweis:

Die Algorithmen **SHA2 256bit** und **SHA2 512bit** benötigen einen hohen Anteil der Systemresourcen.

SA Lifetime (secs): Hier definieren Sie die Dauer der IPSec-Verbindung in Sekunden. Nach der Installation sind standardmäßig 3600 Sekunden (1h) eingestellt.
Generell ist eine Zeitspanne zwischen 60 und 28800 Sekunden möglich.

PFS: Die IPSec-Schlüssel für die IPSec-Verbindung werden auf der Basis von Zufallsdaten generiert. Mit **Perfect Forwarding Secrecy (PFS)** wird sichergestellt, dass diese Zufallsdaten nicht bereits zur Erstellung eines anderen Schlüssels, z. B. für die IKE-Verbindung, verwendet wurden. Falls ein älterer Schlüssel gefunden oder berechnet wird, können daher keinerlei Rückschlüsse auf den neuen Schlüssel gezogen werden.
Die IPSec VPN-Funktion dieses Internet-Sicherheitssystems unterstützt **Group 1 (MODP768)**, **Group 2 (MODP 1024)**, **Group 5 (MODP 1536)**, **Group X (MODP 2048)**, **Group X (MODP 3072)** und **Group X (MODP 4096)**. Wenn Sie **PFS** ausschalten möchten wählen Sie **No PFS** aus.

Per Default ist bei dieser Funktion bereits **Group 5 (MODP 1536)** eingestellt.

Wichtiger Hinweis:

PFS benötigt durch den **Diffie-Hellmann**-Schlüsselaustausch zusätzliche Rechenleistung. **PFS** ist außerdem nicht immer 100%-ig kompatibel unter den verschiedenen Herstellern. Bei Problemen mit der Rechner-Performance oder mit dem Verbindungsaufbau zur Gegenstelle schalten Sie diese Funktion bitte aus.

Compression: Mit Hilfe dieser Algorithmen können Sie die IP-Pakete komprimieren, bevor sie verschlüsselt werden.

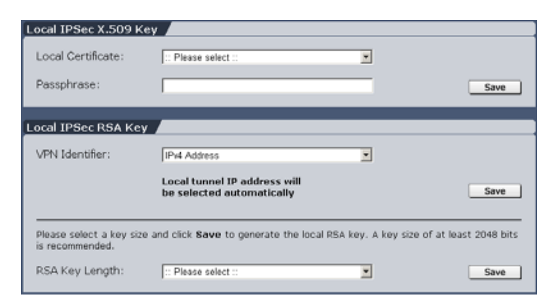
Dieses System unterstützt den Deflate-Algorithmus.

6. Falls Sie für diese IPSec Policy noch keinen Namen definiert haben, tragen Sie nun im Eingabefeld **Name** einen Namen ein.

7. Erzeugen Sie die Policy durch einen Klick auf die Schaltfläche **Add**.

Die neue **Policy** wird anschließend in der Tabelle **IPSec Policies** angezeigt.

5.7.3. Local Keys



Im Menü **Local Keys** verwalten Sie das lokale **X.509**-Zertifikat für die X.509-Authentifizierung, definieren den Local IPSec Identifier und das locale RSA-(Key)-Schlüssel-Paar für die RSA-Authentifizierung.

Local IPSec X.509 Key

In diesem Fenster können Sie für **X.509**-Zertifikate, die Sie zuvor im Menü **IPSec VPN/CA Management** erstellt haben, die lokalen Schlüssel definieren. Das Erstellen der X.509-Zertifikate wird in Kapitel 5.7.6 ab Seite 389 beschrieben.

Local Certificate: Wählen Sie hier das Zertifikat für die **X.509**-Authentifizierung aus. Es sind nur die Zertifikate verfügbar, bei denen der passende **Private Key** vorhanden ist.

Passphrase: Tragen Sie in das Eingabefeld das Passwort ein, mit dem der Private Key gesichert ist.

Der **Active Key** wird anschließend mit seinem Namen im Fenster **Local IPSec X.509 Key** angezeigt. Wenn Sie einen neuen *Local Key* auswählen, wird der alte automatisch ersetzt.

Das Sicherheitssystem verwendet nun die **ID** und den **Public**/**Private Key** des aktuellen *Local X.509 Key* zur Identifizierung, Authentifizierung und zur Verschlüsselung des *X.509 IPSec Key Exchanges*.

RSA Authentication

Für die Authentifizierung mit **RSA** wird an den Endpunkten jeweils ein *Schlüssel-(Key)-Paar* bestehend aus einem **Public Key** (öffentlichen Schlüssel) und einem **Private Key** (privaten Schlüssel) benötigt.
Das Schlüssel-(Key)-Paar wird in zwei Schritten im Fenster **Local IPSec RSA Key** erstellt: Zuerst wird der **Local IPSec Identifier** definiert und daraus wird anschließend das *Schlüssel-(Key)-Paar* generiert.

1. Definieren Sie im Fenster **Local IPSec RSA Key** einen einzigartigen **VPN Identifier**.

   IPv4 Address: Für statische IP-Adressen.

   Hostname: Für VPN Security Gateways mit dynamischen IP-Adressen.

   E-Mail Address: Für mobile Road-Warrior-Verbindungen.

   Speichern Sie anschließend die Einstellung durch einen Klick auf die Schaltfläche **Save**.

2. Generieren Sie einen neuen **RSA Key**, indem Sie im Drop-down-Menü **RSA Key length** die Schlüsselstärke auswählen.

   Wichtiger Hinweis:

   Die **Schlüssellänge** (**Key Length**) muss auf beiden Sicherheitssystem identisch eingestellt werden. Die Generierung der **RSA Keys** kann je nach gewählter Schlüssellänge und der zur Verfügung stehenden Hardware bis zu mehreren Minuten dauern.

3. Starten Sie die Generierung des *Schlüssel-(Key)-Paars* durch einen Klick auf die Schaltfläche **Save**.

Im Fenster **Local Public RSA Key** wird anschließend der aktive **Public Key** angezeigt. Der *Public Key* aus diesem Fenster wird mit der jeweiligen Gegenstelle, z. B. per E-Mail ausgetauscht.

Der **Public Key** von der Gegenstelle wird später im Menü **Remote Keys** in das Fenster **Public Key** eingegeben. Das Menü **Remote Keys** wird in Kapitel 5.7.4 ab Seite 382 beschrieben.

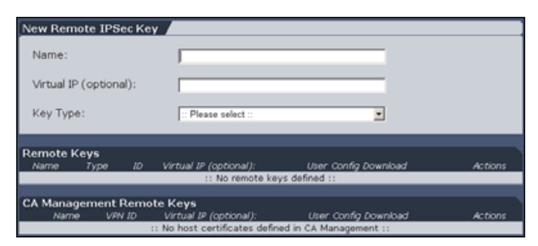
PSK Authentication

Für die Authentifizierung mit **Preshared Keys (PSK)** werden in diesem Menü keine Einstellungen für den **local IPSec Key** benötigt!

Während des *Schlüsselaustauschs* (*Key Exchange*) wird passend zum verwendeten **IKE Main Mode** nur **IPv4 Address** als **IPSec Identifier** unterstützt. Die *IPSec Identifier* werden im *IKE Main Mode* automatisch durch **PSK** verschlüsselt – die Authentifizierung mit **PSK** kann daher nicht verwendet werden. Die IP-Adressen der IKE-Verbindung werden automatisch als **IPSec Identifier** verwendet.

Den **PSK Key** generieren Sie im Menü **IPSec VPN / Remote Keys**. Er wird dann automatisch als **Local PSK Key** eingesetzt.

5.7.4. Remote Keys



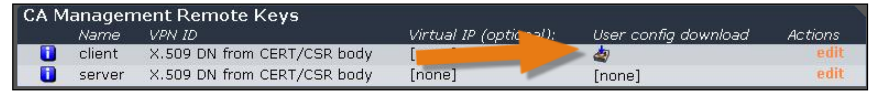
Im Menü **Remote Keys** verwalten Sie die IPSec-Remote-Key-Objekte. Ein IPSec-Remote-Key-Objekt repräsentiert eine IPSec-Gegenstelle. Diese Gegenstelle kann ein **Security Gateway**, ein **Host** oder auch ein **Road Warrior** mit *dynamischer IP-Adresse* sein.

Ein IPSec-Remote-Key-Objekt enthält drei Parameter:

- Die IKE-Authentifizierungsmethode (PSK/RSA/X.509)
- Die IPSec ID der Gegenstelle (IP/Hostname/E-Mail-Adresse/Certificate)
- Die Authentifizierungsdaten (Shared Secret mit PSK, Public Key mit RSA, X.509-Zertifikate werden während dem Key Exchange übermittelt)

User Config Download

Die Funktion **User Config Download** erleichtert die Konfiguration der Client-Anwendungen für X.509-basierte IPSec-VPN-Road-Warrior-Verbindungen. Die Funktion ist in der Tabelle **CA Management Remote Keys** enthalten und wird aktiviert, wenn das entsprechende Benutzerzertifikat im Menü **IPSec VPN/Connections** für eine Road-Warrior-Verbindung ausgewählt wurde.



Das Sicherheitssystem speichert das Profil der X.509-basierten Road-Warrior-Verbindung in einer INI-Datei. Durch einen Klick auf das Download-Symbol ( ) können Sie diese INI-Datei herunterladen und in eine IPSec-Client-Anwendung mit entsprechender *Profil-Import-*

Funktion (z. B. **Astaro Secure Client V8.3**) einlesen.
Die *User-Config*-Datei enthält als Ausweichlösung die Standard-Algorithmen, falls für die IPSec-VPN-Verbindung eine Verschlüsselung oder ein Authentisierungs-Algorithmus eingestellt wurde, der von der IPSec-Client-Anwendung nicht unterstützt wird.

Beachten Sie, dass Sie für die Konfiguration des *Road Warrior Clients* auch die Container-Datei **PKCS#12** mit den Zertifikaten benötigen. Die Container-Datei wird im Menü IPSec **VPN/CA Management** erstellt und kann dort auch heruntergeladen werden. Das Menü **CA Management** wird in Kapitel 5.7.6 ab Seite 389 beschrieben.



Das Einrichten des **Astaro Secure Client V8.3** wird im zugehörigen *Benutzerhandbuch* und im *Configuration Guide* beschrieben. Sie finden die aktuellen Handbücher und Guides unter der Internetadresse **http://www.astaro.com/kb**.

New Remote IPSec Key

Für jede IPSec-VPN-Gegenstelle muss ein **IPSec-Remote-Key**-Objekt definiert werden. Die neuen *Remote-Key*-Objekte werden im Fenster **Remote IPSec Key** definiert.

IPSec Remote Key definieren:

1. Öffnen Sie im Verzeichnis **IPSec VPN** das Menü **Remote Keys**.

   Das Fenster **New Remote IPSec Key** wird angezeigt.

2. Tragen Sie in das Eingabefeld **Name** einen Namen für den neuen **Remote Key** ein.

   Wenn Sie den *IPSec Remote Key* für eine Standard-Verbindung konfigurieren, fahren Sie mit Schritt 3 fort.

   Virtual IP (optional): Mit dieser Funktion können Sie einem Road Warrior eine virtuelle IP-Adresse zuweisen. Dies ist die einzige Methode eine virtuelle IP-Adresse manuell auszutauschen.

Wenn Sie in das Eingabefeld eine IP-Adresse eintragen, dann muss diese auch auf dem Road Warrior eingetragen werden.

Achtung:

Die Funktion **Virtual IP** muss eingeschaltet werden, wenn Sie für den IPSec-Tunnel mit einem Road Warrior die Funktion **NAT Traversal** verwenden und **L2TP Encapsulation** ausgeschaltet ist. Die hier eingetragene IP-Adresse darf sonst nirgends verwendet werden und darf nicht Teil eines angeschlossenen Sub-Netzwerks sein.

3. Wählen Sie im Drop-down-Menü **Key Type** die IKE-Authentifizierungsart aus. Die weiteren Einstellungen richten sich nach dem ausgewählten **Key Type**.

PSK: Während des Key Exchange wird passend zum verwendeten **IKE Main Mode** nur **IPv4 Address** als **VPN Identifier** der Gegenstelle unterstützt. Tragen Sie in das Eingabefeld **Preshared Key** ein Passwort ein.
Falls Sie mehrere Road-Warrior-Verbindungen konfigurieren möchten, benötigen Sie für alle Verbindungen nur einen *PSK*.



Sicherheitshinweis:

Setzen Sie sichere Passwörter! Ihr Vorname rückwärts buchstabiert ist beispielsweise kein ausreichend sicheres Passwort – besser wäre z. B. xfT35!4z. Stellen Sie sicher, dass dieses Passwort nicht in unbefugte Hände fällt. Der Inhaber dieses Passworts kann damit eine VPN-Verbindung in das geschützte Netzwerk aufbauen. Es ist empfehlenswert das Passwort in regelmäßigen Abständen zu wechseln.

RSA: Das Schlüsselpaar besteht aus einem **Privat Key** und einem **Public Key**. Damit Sie mit der Gegenstelle kommunizieren können, müssen Sie jeweils die **Public Keys** austauschen. Der Austausch der **Public Keys** kann per E-Mail erfolgen.

Wählen Sie im Drop-down-Menü **VPN Identifier** den VPN-ID-Type der Gegenstelle aus. Bei den Optionen **E-Mail Address**, **Full qualified domain name** und **IP Address** müssen Sie die zugehörige Adresse oder den Namen in das darunter liegende Eingabefeld eintragen.

X.509: Wählen Sie im Drop-down-Menü **VPN Identifier** den VPN-ID-Type aus. Bei den Optionen **E-Mail Address**, **Full qualified Domain Name** oder **IP Address** müssen Sie die zugehörige Adresse oder den Namen in das darunter liegende Eingabefeld eintragen.

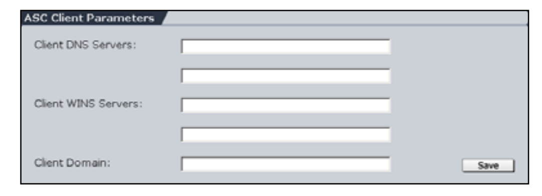
Für den VPN-ID-Type **Distinguished Name** benötigen Sie die folgenden Daten aus dem X.509-Verzeichnisbaum: Country (C), State (ST), Local (L), Organization (O), Unit (UO), Common Name (CN) und E-Mail Address (E-Mai).

4. Um das neue IPSec-Remote-Key-Objekt zu übernehmen, klicken Sie auf die Schaltfläche **Add**.

Das neue IPSec-Remote-Key-Objekt wird anschließend in der Tabelle **Remote Keys** angezeigt.

Die **CA Management Remote Keys** werden in einer separaten Tabelle angezeigt.

ASC Client Parameters



In diesem Fenster können Sie den Clients während des Verbindungsaufbaus zusätzlich bestimmte Name-(DNS)- und WINS-Server sowie eine Client Domain zuweisen.

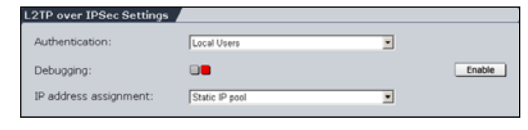
5.7.5. L2TP over IPSec

L2TP over IPSec ist eine Kombination des *Layer 2 Tunneling Protocol* und des Standardprotokolls *IPSec*. Mit **L2TP over IPSec** können Sie mit der gleichen Funktionalität wie PPTP einzelnen Hosts über einen verschlüsselten IPSec-Tunnel den Zugang zu Ihrem Netzwerk ermöglichen. **L2TP over IPSec** ist einfach einzurichten und benötigt auf Microsoft Windows XP Clients keine zusätzliche Software.

Für die MS-Windows-Systeme 98, ME und NT Workstation 4.0 muss der **Microsoft L2TP/IPSec VPN Client** aufgespielt werden. Diesen Client finden Sie bei Microsoft unter:

http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/l2tpclient.asp

L2TP over IPSec Settings

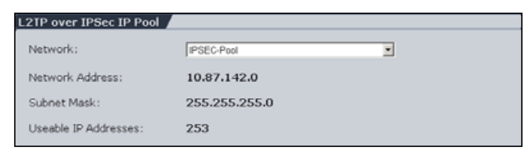


Authentication: In diesem Drop-down-Menü stellen Sie die Authentifizierungsmethode ein. Wenn Sie im Menü **System/User Authentication** einen RADIUS-Server konfiguriert haben, können Sie hier auch RADIUS-Authentifizierung einsetzen.
Die Konfiguration des Microsoft IAS RADIUS-Servers und die Einstellungen im WebAdmin werden in Kapitel 5.1.8 ab Seite 83 erklärt.

Debugging: Diese Funktion steht Ihnen zur Überprüfung der L2TP-over-IPSec-Verbindung zur Verfügung. In den IPSec Logs werden ausführliche Informationen protokolliert. Diese Protokolle können Sie im Menü **Local Logs/Browse** in Echtzeit beobachten oder auf Ihren lokalen Rechner herunterladen. Die Funktionen im Menü **Local Logs** werden im Kapitel 5.10 ab Seite 417 beschrieben.

IP Address Assignment: Mit dieser Funktion können Sie festlegen, ob den Hosts bei der Einwahl eine Adresse aus einem definierten **L2TP over IPSec IP Pool** zugewiesen werden soll, oder ob die Adresse automatisch von einem **DHCP**-Server angefordert wird.
Bitte beachten Sie, dass der *lokale DHCP-Server* für diese Funktion nicht unterstützt wird. Der DHCP-Server muss physikalisch auf einem anderen System laufen.

L2TP over IPSec IP Pool

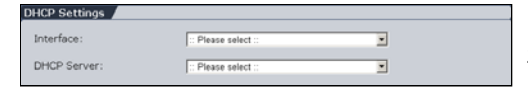


Hier legen Sie fest, welche IP-Adressen den Hosts bei der Einwahl zugewiesen werden. Per Default-Einstellung wird beim ersten Aktivieren der L2TP-over-IPSec-Funktion ein Netzwerk aus dem privaten IP-Bereich 10.x.x.x ausgewählt. Dieses Netzwerk wird **IPSec Pool** genannt und kann für alle anderen Funktionen des Internet-Sicherheitssystems genutzt werden, in denen Netzwerkdefinitionen verwendet werden. Falls Sie ein anderes Netzwerk verwenden wollen, können Sie entweder die bestehende *IPSec-Pool*-Definition verändern, oder ein anderes definiertes Netzwerk als *IPSec Pool* festlegen.

Hinweis:

Falls Sie für Ihren **IPSec Pool** private IP-Adressen, wie z. .B. das vordefinierte Netzwerk verwenden, müssen Sie **Masquerading** oder **NAT**-Regeln für den *IPSec Pool* erstellen, wenn ein Zugriff auf das Internet von den IPSec-Hosts aus erwünscht ist.

DHCP Settings

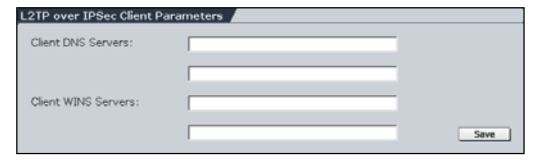


Dieses Fenster wird angezeigt, wenn Sie im Fenster **L2TP over IPSec Settings** bei der Funktion **IP Address Assignment** die Einstellung **DHCP** ausgewählt haben.

Interface: Stellen Sie hier die Netzwerkkarte ein, über die der DHCP-Server angeschlossen ist. Beachten Sie dabei, dass der DHCP-Server nicht direkt angeschlossen sein muss – der Zugang ist ebenso über einen Router möglich.

DHCP Server: Wählen Sie hier den DHCP-Server aus. In diesem Drop-down-Menü werden alle Hosts angezeigt, die im Menü **Definitions/Networks** definiert wurden.

L2TP over IPSec Client Parameters



In diesem Fenster können Sie den Hosts während des Verbindungsaufbaus zusätzlich bestimmte Name- (DNS)- und WINS-Server zuweisen.

5.7.6. CA Management

Certificate Authority (CA) ist die Ausgabestelle von Zertifikaten für öffentliche Schlüssel. Im Menü **CA Management** können Sie Ihre eigene **X.509 Certificate Authority (CA)** erstellen und verwalten. Diese werden bei einer IPSec-Verbindung zur Authentifizierung der Benutzer an den beiden Gegenstellen verwendet. Die dafür verwendeten Informationen sind in den X.509-Zertifikaten gespeichert.
Sie können aber auch Zertifikate verwenden, die von kommerziellen Anbietern, z. B. VeriSign signiert wurden.

Hinweis:

Jedes Zertifikat ist in der **CA** hinsichtlich der darin verwendeten Informationen (Name, Firma, Ort, usw.) eindeutig. Es kann kein zweites Zertifikat mit dem gleichen Inhalt erzeugt werden - auch nicht, wenn das Erste zuvor gelöscht wurde.

Mit dem Menü **CA Management** sind Sie in der Lage, drei verschiedene Zertifikats-Typen zu verwalten. Diese können wiederum für verschiedene Zwecke eingesetzt werden. Dies hängt davon ab, ob jeweils der **Private Key** mit abgespeichert wurde:

CA (Certificate Authority) Certificate: Wenn ein **CA** ohne **Private Key** gespeichert wird, kann dieses bei ankommenden IPSec-Verbindungen zur Authentifizierungsüberprüfung des Host- und Benutzer-Zertifikats verwendet werden. Ein solches **CA** wird als **Verification CA** bezeichnet.
Wenn im **CA** ein **Private Key** vorhanden ist, kann es zum Signieren von Zertifikatsanfragen verwendet werden, um daraus ein gültiges Zertifikat zu erstellen. Dieses **CA** wird dann **Signing CA** genannt.
Auf Ihrem System können mehrere **Verfication CAs** vorhanden sein, allerdings nur ein **Signing CA**.

Host CSR (Certificate Signing Request): Dies ist eine Zertifikats-Anfrage von einem Host. Wenn Sie die Anfrage mit einem **Signing CA** signieren, wird der **Host CSR** zu einem gültigen Host-Zertifikat.

Host Certificate: Das Zertifikat beinhaltet den **Public Key** des Hosts sowie Informationen durch die der Host identifiziert wird, z. B. die IP-Adresse oder den Benutzer. Das Zertifikat ist außerdem durch eine **CA** signiert, die sicherstellt, dass der **Key** auch tatsächlich zu den angegebenen Informationen passt. Dieses gültige Zertifikat wird zur Authentifizierung eines Remote IPSec Hosts/Benutzers verwendet.



Mit Hilfe des Drop-down-Menüs in der Fußzeile der Tabellen können Sie die Zertifikate in verschiedenen Dateiformaten auf Ihren lokalen Client herunterladen oder Zertifikate auf dem System löschen:

PEM: Ein ASCII-codiertes Format. Das Zertifikat bzw. die Anfrage und der Private Key werden in separaten Dateien gespeichert.

DER: Ein binärcodiertes Format. Das Zertifikat bzw. die Anfrage und der Private Key werden in separaten Dateien gespeichert.

PKCS#12: Ein Container-File. Diese Datei kann das Zertifikat, den Private Key und den Authentication CA beinhalten.

Delete: Die ausgewählten Zertifikate werden aus der Tabelle gelöscht.

Issue CERT from CSR: Mit dieser Funktion wird aus dem **CSR** das Zertifikat generiert.

Client / Host-Zertifikat erstellen:

Schritt 1: Das **Signing CA** erstellen.

1. Öffnen Sie im Verzeichnis **IPSec VPN** das Menü **CA Management**.

2. Klicken Sie in der Tabelle **Certificate Authorities** auf die Schaltfläche **New**.

   Anschließend öffnet sich das Fenster **Add Certificate Authority**.

3. Wählen Sie die Option **Generate** aus.

4. Vergeben Sie im Eingabefeld **Name** einen eindeutigen **Namen** für das Zertifikat.

   Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9 und Unterstrich.

5. Tragen Sie in das Eingabefeld **Passphrase** ein Passwort mit mindestens vier Zeichen ein.

6. Wählen Sie im Drop-down-Menü **Key Size** die Verschlüsselungsstärke aus.

7. Tragen Sie in die Drop-down-Menüs und Eingabefelder **Country** bis **E-Mail Address** die Authentifizierungsdaten für dieses **CA** ein.

8. Um die Einträge zu speichern Klicken Sie auf die Schaltfläche **Start**.

Anschließend wird die **Signing CA** in die Tabelle **Certificate Authorities** geladen. Diese CA wird nun dazu verwendet, um Zertifikats-Anträge (**CSR**) zu signieren und dann daraus ein Zertifikat zu erstellen.

Schritt 2: Den **Zertifikats-Antrag (Request)** erstellen.

1. Klicken Sie in der Tabelle **Host CSR or Certificate** auf die Schaltfläche **New**.

   Anschließend öffnet sich das Fenster **Add Host CSR or Certificate**.

2. Wählen Sie die Option **Generate CSR** aus.

   Wählen Sie im Drop-down-Menü **VPN ID** den VPN-ID-Type aus. Bei den Optionen **E-Mail Address**, **Hostname** und **Ipv4 Address** müssen Sie den zugehörigen Wert in das rechte Eingabefeld eintragen.
   Bei der Option **X.509 DN** bleibt das rechte Feld leer.

3. Vergeben Sie im Eingabefeld **Name** einen eindeutigen **Namen** für den Zertifikats-Antrag.

   Erlaubte Zeichen sind: Das Alphabet, die Zahlen 0 bis 9 und Unterstrich.

4. Tragen Sie in das Eingabefeld **Passphrase** ein Passwort mit mindestens vier Zeichen ein.

5. Wählen Sie im Drop-down-Menü **Key Size** die Verschlüsselungsstärke aus.

6. Tragen Sie in die Drop-down-Menüs und Eingabefelder **Country** bis **E-Mail Address** die Authentifizierungsdaten für dieses **CSR** ein.

   Common Name: Wenn Sie dieses CSR für eine Road-Warrior-Verbindung erstellen möchten, tragen Sie in dieses Feld den Namen des Benutzers (User) ein. Für die Verbindung zu einem Host tragen Sie hier den Hostnamen ein.

7. Um die Einträge zu speichern klicken Sie auf die Schaltfläche **Start**.

Anschließend wird der Zertifikats-Antrag **CSR + KEY** in die Tabelle **Host CSRs and Certificates** geladen. In der Tabelle wird der Type,

der Name und die VPN ID angezeigt. Diese Anfrage kann nun mit der **Signing CA** aus Schritt 1 signiert werden.

Schritt 3: Das Zertifikat erstellen.

1. Wählen Sie in der Tabelle **Host CSRs and Certificates** den neu erstellten Zertifikats-Antrag **CSR + KEY** aus.
2. Wählen Sie im Drop-down-Menü in der Fußzeile der Tabelle die Funktion **Issue CERT from CSR** aus.

   Anschließend wird das Eingabefeld **Signing CA Passphrase** sichtbar. Tragen Sie hier das Passwort der **Signing CA** ein.
3. Klicken Sie auf die Schaltfläche **Start**.

Anschießend wird aus dem Antrag **CSR + KEY** das fertige Zertifikat **CERT + KEY** erstellt und in der Tabelle entsprechend ausgetauscht.

Schritt 4: Zertifikat herunterladen.

1. Wählen Sie in der Tabelle **Host CSRs and Certificates** das neue Zertifikat aus.
2. Wählen Sie im Drop-down-Menü in der Fußzeile der Tabelle ein Download-Format aus.

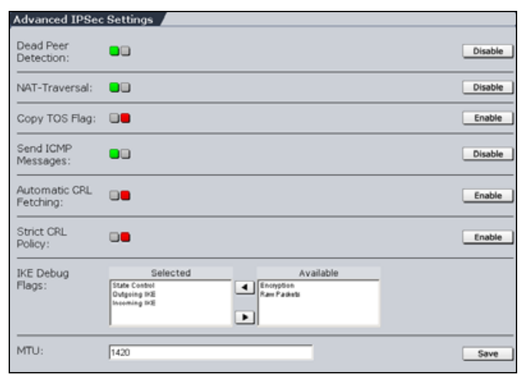
   DER: Tragen Sie in das Eingabefeld **Passphrase** das Passwort des **Privat Key** ein.

   PEM: Für dieses Format wird kein Passwort benötigt.

   PKCS#12: Tragen Sie in das Eingabefeld **Passphrase** das Passwort des **Private Key** ein. In das Eingabefeld **Export Pass** geben Sie ein zusätzliches Passwort ein. Dieses Passwort benötigen Sie oder ein anderer Benutzer, um das Zertifikat auf dem externen Client zu importieren.
3. Klicken Sie auf die Schaltfläche **Start**.

Das Zertifikat muss nun auf dem externen IPSec VPN-Client installiert werden. Der Installationsablauf hängt von der IPSec-Software ab, die auf diesem Client verwendet wird.

5.7.7. Advanced



In diesem Menü können Sie für das Modul **IPSec VPN** zusätzliche Einstellungen durchführen. Diese sollten allerdings nur von erfahrenen Benutzern durchgeführt werden.

Dead Peer Detection: Diese Funktion ermittelt automatisch, ob der VPN-Gateway oder der Client auf der gegenüberliegenden Seite noch erreichbar ist. Bei Verbindungen mit statischen Endpunkten wird der Tunnel nach einem Ausfall automatisch neu ausgehandelt. Für Verbindungen mit dynamischen Endpunkten wird für eine neue Aushandlung des Tunnels die Gegenstelle benötigt. In der Regel ist diese Funktion betriebssicher und kann immer eingeschaltet bleiben, unabhängig davon, ob die Gegenstelle *Dead Peer Detection* unterstützt. Die Funktion wird automatisch ausgehandelt.

NAT Traversal: Wenn diese Funktion eingeschaltet ist, können Hosts einen IPSec-Tunnel durch *NAT-Geräte* aufbauen. Diese Funktion versucht zu ermitteln, ob zwischen Server und Client *NAT-Geräte* verwendet werden. Wenn *NAT-Geräte* entdeckt werden, verwendet das System zur Kommunikation mit dem externen Host UDP-Pakete. Dies funktioniert allerdings nur, wenn beide IPSec-Endpunkte *NAT Traversal* unterstützen und auf dem Road-Warrior-Endpunkt eine *virtuelle IP-Adresse* eingestellt ist.
Zusätzlich muss auf dem *NAT-Gerät* der IPSec-Passthrough ausgeschaltet sein, da dies *NAT Traversal* unterbrechen kann.

Wichtiger Hinweis:

Für die Funktion **Virtual IP** können keine lokalen IP-Adressen verwendet werden, da das Internet-Sicherheitssystem keine ARP-Anfragen für diese Adressen beantwortet.

Copy TOS Flag: Die **Type-of-Service**-Bits (**TOS**) sind eine Menge von vier Bit-Flags im IP-Header. Die Bits werden *Type-of-Service*-Bits genannt, da sie es der übertragenden Applikation ermöglichen, dem Netzwerk mitzuteilen, welche Art von Dienstgüte gerade benötigt wird. Die verfügbaren Dienstgüteklassen sind: Minimale Verzögerung (minimum delay), maximaler Durchsatz (maximum throughput), maximale Zuverlässigigkeit (maximum reliability) und minimale Kosten (minimum cost).
Mit dieser Funktion wird der Inhalt des **Type-of-Service**-Feldes in das verschlüsselte Datenpaket kopiert. Auf diese Weise kann der IPSec-Datenverkehr aufgrund seiner Priorität geroutet werden.
Die Funktion **Copy TOS Flag** wird durch einen Klick auf die Schaltfläche **Enable** eingeschaltet.

Send ICMP Messages: Falls ein Datenpaket den eingestellten **MTU**-Wert überschreitet, wird vom System eine ICMP-Nachricht an die Quelladresse gesendet: Destination unrechable/fragmentation needed (Zieladresse nicht erreichbar/Fragmentierung erforderlich).
Dies ermöglicht die Verwendung von Path MTU Discovery.

Automatic CRL Fetching: Es sind Situationen denkbar, in denen ein Zertifikataussteller noch während der Gültigkeitsdauer eines Zertifikats die darin gegebene Bestätigung für ungültig erklären möchte, z. B. weil zwischenzeitlich bekannt wurde, dass das Zertifikat vom Zertifikatnehmer unter Angabe falscher Daten (Name usw.) erschlichen wurde oder weil der zum zertifizierten öffentlichen Schlüssel gehörende geheime Schlüssel einem Angreifer in die Hände gefallen

ist. Zu diesem Zweck werden sogenannte *Zertifikatwiderrufslisten*, bzw. **Certificate Revocation Lists** (**CRL**) verwendet. Diese enthalten üblicherweise die Seriennummern derjenigen Zertifikate einer Zertifizierungsinstanz, die für ungültig erklärt werden und deren regulärer Gültigkeitszeitraum noch nicht abgelaufen ist.
Nach Ablauf dieses Zeitraumes besitzt das Zertifikat in jedem Fall keine Gültigkeit mehr und muss daher auch nicht weiter auf der Zertifikatswiderrufsliste geführt werden.

Mit der Funktion **Automatic CRL Fetching** erfolgt die Abfrage der *CRL* automatisch über die URL die im Partnerzertifikat festgelegt ist via HTTP, Anonymous FTP oder LDAP Version 3. Die *CRL* wird auf Anfrage heruntergeladen, abgespeichert und upgedated sobald der Gültigkeitszeitraum abgelaufen ist.
Die Funktion wird durch einen Klick auf die Schaltfläche **Enable** eingeschaltet (Statusampel zeigt Grün).

Achten Sie darauf, dass die Paketfilterregeln im Menü **Packet Filter/ Rules** so gesetzt sind, dass auf den **CRL Disribution Server** zugegriffen werden kann.

Strict CRL Policy: Jedes Partnerzertifikat, das keine entsprechende *CRL* verfügbar hat wird abgelehnt.
Die Funktion wird durch einen Klick auf die Schaltfläche **Enable** eingeschaltet (Statusampel zeigt Grün).

IKE debug Flags: Mit diesem Auswahlfeld können Sie den Umfang der IKE-Debugging-Protokolle einstellen. Im Menü **IPSec VPN/Connections** muss die Funktion IKE Debugging eingeschaltet sein.

Die folgenden Flags können protokolliert werden:

- State Control: Kontrollnachrichten zum IKE-Status
- Encryption: Verschlüsselungs- und Entschlüsselungsoperationen
- Outgoing IKE: Inhalte von ausgehenden IKE-Nachrichten

- Incoming IKE: Inhalte von eingehenden IKE-Nachrichten
- Raw Packets: Nachrichten in unverarbeiteten bytes

MTU: Tragen Sie in das Eingabefeld den MTU-Wert ein.
Per Default ist bereits ein MTU-Wert definiert: 1420 Byte.

5.8. System Management (Reporting)

Über das **Reporting** können Sie sich im Internet-Sicherheitssystem aktuelle Systeminformationen und Systemzustände anzeigen lassen sowie verschiedene Protokollfunktionen in Echtzeit öffnen. Die dargestellten Werte werden alle 5 Minuten aktualisiert.

Alle Diagramme im Verzeichnis **Reporting** zeigen im ersten Schritt einen Überblick der tagesaktuellen Auslastung. Durch einen Klick auf die Schaltfläche **Show all ...** öffnen Sie ein Zusatzfenster mit den wöchentlichen, monatlichen oder jährlichen Durchschnittswerten.

5.8.1. Administration

Report: Administrative Statistics

	Today	Yesterday	Last 7 Days	Last 30 Days
WebAdmin logins (success/failed)	0 / 0	0 / 0	5 / 0	10 / 0
Remote logins (success/failed)	0 / 0	0 / 0	0 / 0	0 / 0
Local logins (success/failed)	0 / 0	0 / 0	0 / 0	1 / 0
Up2Date: System (success/failed)	0 / 0	0 / 0	0 / 0	0 / 0
Up2Date: Virus Protection (success/failed)	20 / 0	25 / 0	148 / 3	217 / 8
Up2Date: Spam Protection (success/failed)	0 / 0	0 / 0	1 / 0	2 / 0
Up2Date: Intrusion Protection (success/failed)	0 / 0	0 / 0	1 / 0	2 / 0
Config changes (total)	0	0	4	33
ACM uploads (total)	0	0	0	0
System restarts (total)	0	0	0	1
HA takeover (total)	0	0	0	0
Uplink failover events (total)	0	0	0	0

License usage (Daily Graph)

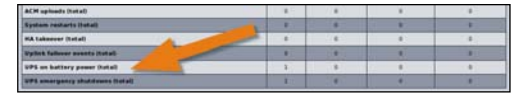
Show all license usage graphs

Das Menü **Administration** enthält eine Übersicht mit administrativen Ereignissen der letzten 30 Tage.

Die folgenden Vorgänge werden angezeigt:

- WebAdmin Logins
- Remote Logins
- Local Logins
- Up2Date: System
- Up2Date: Virus Protection

- Up2Date: Intrusion Protection
- Config Changes
- Astaro Configuration Manager Uploads
- System Restarts
- High Availability Takeover
- Uplink Failover Events



ACM uploads (total)	0	0	0	0
System restarts (total)	0	0	0	0
HA takeover (total)	0	0	0	0
Uplink failover events (total)	0	0	0	0
UPS on battery power (total)	1	0	0	0
UPS emergency shutdowns (total)	1	0	0	0

Die folgenden beiden Zeilen werden angezeigt, wenn die Spannungsversorgung des Sicherheitssystems durch ein **UPS**-Gerät geschützt ist:

- UPS on Battery Power
- UPS Emergency Shut downs

Weitere Informationen zum **UPS-Geräte-Support** erhalten Sie in Kapitel 3.1 auf Seite 22.

5.8.2. Virus Protection

Report: Virus Protection Statistics

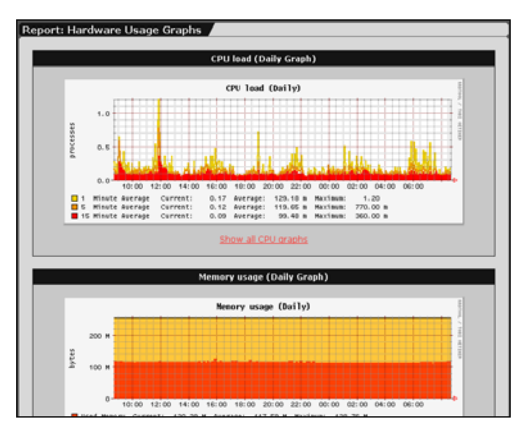
	Today	Yesterday	Last 7 Days	Last 30 Days
SMTP viruses	0	0	0	0
POP3 viruses	0	0	0	0
HTTP viruses	0	0	0	0

Das Menü **Virus Protection** enthält eine Übersicht der gefilterten Viren der letzten 30 Tage.

Die folgenden Viren werden angezeigt:

- SMTP Viruses
- POP3 Viruses
- HTTP Viruses

5.8.3. Hardware



In diesem Menü werden die aktuellen Werte Ihrer System-Hardware angezeigt. Die verfügbaren Werte sind die CPU-Auslastung sowie die RAM und SWAP-Auslastung.

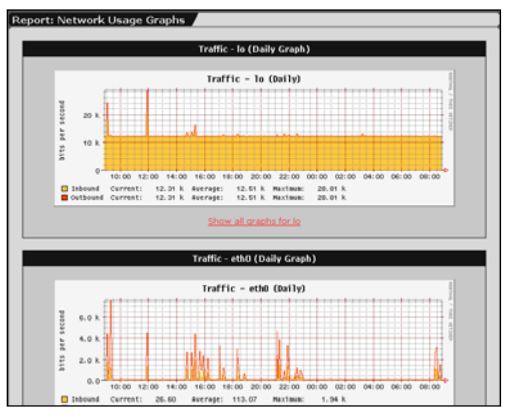
Die Grafiken und Tabellen werden alle fünf Minuten aktualisiert. Die Informationen können durch einen Klick auf die Schaltfläche **Reload** auch manuell aktualisiert werden. Verwenden Sie für die Aktualisierung nicht die Schaltfläche **Aktualisieren** im Browser, da Sie sonst aus dem Konfigurationstool **Web-Admin** ausgeloggt werden!

CPU Load (Daily Graph): Das Diagramm zeigt die aktuelle Auslastung des Prozessors durch das Internet-Sicherheitssystem an.

Memory Usage (Daily Graph): Hier wird die Gesamtsumme des genutzten Hauptspeichers dargestellt. Je mehr Funktionen zur selben Zeit ausgeführt werden, umso weniger freier Hauptspeicher steht zur Verfügung.

SWAP Usage (Daily Graph): Das Diagramm stellt die aktuelle Nutzung des virtuellen Speichers dar. Verfügt Ihr System über sehr wenig Hauptspeicher (**RAM**) wird die SWAP-Nutzung stark ansteigen.

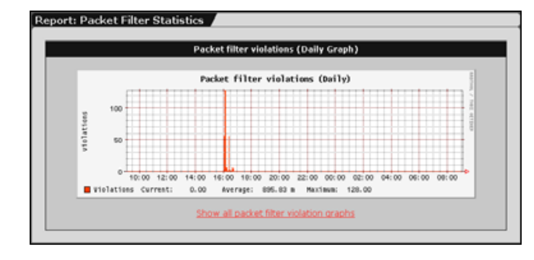
5.8.4. Network



In diesem Menü wird die Datenverkehr-Auslastung der einzelnen Schnittstellen grafisch dargestellt. Voraussetzung für dieses Reporting ist, dass alle Netzwerkkarten unter **Network/Interfaces** korrekt konfiguriert wurden.

Die Konfiguration der Netzwerkkarten wird in Kapitel 5.3.2 ab Seite 154 beschrieben.

5.8.5. Packet Filter



In diesem Menü werden die Paketfilterregelverletzungen in Diagrammen grafisch dargestellt. Die Regelverletzungen werden auch in den **Packet Filter Logs** protokolliert. Die Log-Dateien befinden sich im Menü **Local Logs/Browse**.

5.8.6. Content Filter

In diesem Menü werden zu den Proxies HTTP, SMTP und POP3 die ausgewerteten Daten und Ereignisse des **Content Filter** in Form von Tabellen und Diagrammen angezeigt. Das Modul **Spam Protection** und der **Spam Score** werden im Kapitel 5.6.2.2 ab Seite 320 erklärt.

Informationen zu den Proxies SMTP und POP3:

- Summe der bearbeiteten Nachrichten
- Die durchschnittliche Größe der Nachrichten in Kilobytes
- Die durchschnittliche Höhe des *Spam Score*

Informationen zum Proxy HTTP:

- Summe der angefragten HTTP-Seiten
- Summe der durch *Surf Protection* geblockten HTTP-Seiten
- Summe der durch *Virus Protection for Web* geblockten HTTP-Seiten
- Summe der durch *Spyware Protection* geblockten HTTP-Seiten

5.8.7. PPTP/IPSec VPN

In diesem Menü werden die PPTP- und die IPSec-VPN-Verbindungen grafisch dargestellt.

5.8.8. Intrusion Protection

In diesem Menü werden die Intrusion-Protection-Vorfälle grafisch dargestellt.

5.8.9. DNS

In diesem Menü wird die DNS-Query-Statistik dargestellt.

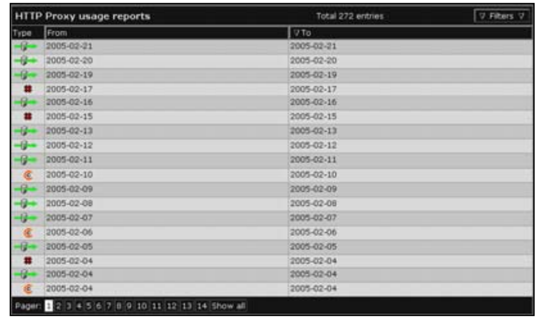
5.8.10. SIP

In diesem Menü wird der Zugriff auf den **SIP-Proxy** protokolliert. Jede Zeile enthält vier Spalten indenen die Summe der Ereignisse am heutigen Tag, am gestrigen Tag, an den letzten sieben Tagen und an den letzten 30 Tagen anzeigt werden.

Die folgenden drei Ereignisse werden angezeigt:

- Incoming Call Requests: Die Summe der eingegangenen Anfragen.
- Outgoing Call Requests: Die Summe der ausgegangenen Anfragen.
- Successful Calls: Die Gesamtsumme aller erfolgreich aufgebauten Anrufe.

5.8.11. HTTP Proxy Usage



In diesem Menü wird der Zugriff auf den **HTTP-Proxy** protokolliert.

Wenn Sie im HTTP-Proxy User Authentication eingeschaltet haben, werden im Protokoll Einzelheiten zum Benutzernamen angezeigt.

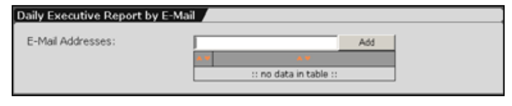
Es gibt drei Protokoll-Typen:

- **Erlaubte Seiten** ( ): Diese Protokolle enthalten Internetseiten, die durchgelassen wurden.
- **Blockierte Seiten** ( ): Diese Protokolle enthalten Internetseiten, die vom *Content Filter* blockiert wurden.
- **Blockierte Categories** ( ): Diese Protokolle enthalten Internetseiten, die von *Surf Protection Categories* blockiert wurden.

5.8.12. Executive Report

Im Menü **Executive Report** wird aus den einzelnen Berichten im Verzeichnis **Reporting** ein Gesamtbericht zusammengestellt.

Daily Executive Report by E-Mail

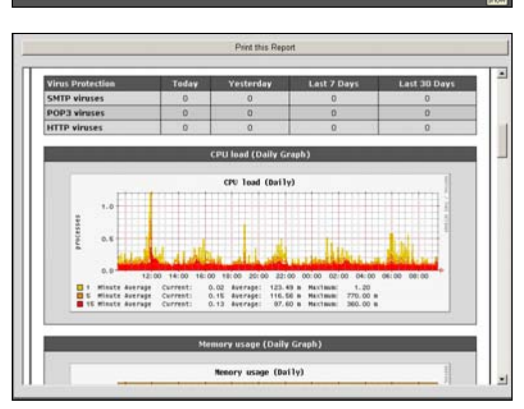


Einmal pro Tag wird ein aktualisierter Gesamtbericht an die im **Hierarchiefeld** eingetragenen E-Mail-Adressen geschickt. Die Funktion wird automatisch aktiviert, sobald im Feld eine Adresse eingetragen ist.

Neue E-Mail-Adressen werden vom Eingabefeld durch einen Klick auf die Schaltfläche **Add** in das Hierarchiefeld übernommen.

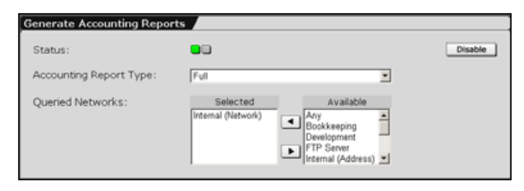
Die Funktionsweise des **Hierarchiefeldes** wird in Kapitel 4.3.5 ab Seite 43 beschrieben.

Current Report



Durch einen Klick auf die Schaltfläche **Show** öffnen Sie ein Fenster mit dem aktuellen Gesamtbericht. Der Bericht kann ausgedruckt werden, indem Sie auf die Schaltfläche **Print this Report** klicken.

5.8.13. Accounting



Mit der Funktion **Accounting** werden auf den Netzwerkkarten alle IP-Pakete erfasst und ihre Größe einmal am Tag aufsummiert. Zusätzlich wird zu Beginn eines Monats die Datensumme des vergangenen Monats berechnet. Das Ergebnis wird in einem Protokoll ausgegeben. Die Summe dient z. B. als Basis für den Betrag, den Ihnen Ihr Internet Service Provider in Rechnung stellt, wenn Sie Ihre Verbindung nach übertragenem Datenvolumen bezahlen.

Das **Accounting** wird im Menü **Network/Accounting** eingeschaltet und konfiguriert. Die Konfiguration dieser Funktion wird im Kapitel 5.3.8 ab Seite 220 beschrieben.

Browse Accounting Reports: In diesem Fenster werden die vorhandenen Accounting-Protokolle angezeigt. Mit dem Drop-down-Menü **Select Report** wählen Sie den Monat aus. Das Protokoll wird anschließend im darrunterliegenden Fenster angezeigt.

Im Menü **Local Logs/Browse** können die Protokolle auf Ihren lokalen Rechner heruntergeladen oder gelöscht werden.

Report for current Month: In diesem Fenster wird das Accounting-Protokoll des aktuellen Monats angezeigt.

Accounting definieren:

1. Öffnen Sie im Verzeichnis **Reporting** das Menü **Accounting**.

2. Schalten Sie die Funktion **Accounting Reports** durch einem Klick auf die Schaltfläche **Enable** ein.

   Anschließend wird das Eingabefenster geöffnet.

3. Wählen Sie im Auswahlfeld unter dem Fenster **Queried Networks** die Netzwerke aus, für die ein detailliertes Protokoll erstellt werden soll. In der Regel ist dies Ihr LAN- und/oder das DMZ-Netzwerk.

   Die Funktionsweise des **Auswahlfeldes** wird in Kapitel 4.3.2 ab Seite 41 beschrieben.

   Wichtiger Hinweis:

   Stellen Sie im Auswahlfeld **Queried Networks** nicht **Any** ein, da dies zur Folge hat, dass alle Quell- und Zielnetzwerke behandelt werden. Dies bedeutet, dass kein Accounting erfogt!

Die Netzwerke werden sofort übernommen und erscheinen anschließend im Fenster **Queried Networks**.

5.8.14. Advanced

RAID Status

Das Fenster wird angezeigt, wenn die Software auf einer Hardware mit einem RAID-Festplattensystem installiert ist. Mit einem RAID-System (Redundant Array of Independent Disks) werden mehrere physikalische Festplatten zu einem besonders leistungsfähigen logischen Laufwerk zusammengefasst.

Achtung:

Damit das **RAID**-System erkannt und in diesem Menü angezeigt wird, benötigen Sie einen RAID-Controller der vom Sicherheitssystem unterstützt wird. Die **Hardware Compatibility List (HCL)** befindet sich auf **www.astaro.com/kb**. Mit Hilfe des Suchbegriffs **HCL** gelangen Sie schnell auf die entsprechende Seite.
Achten Sie beim Austausch einer Festplatte besonders darauf, dass Sie die defekte Festplatte entfernen, da sonst das gesamte RAID-System ausfällt. Achten Sie ebenfalls darauf, dass Sie nur die für das System passende Festplatte vom gleichen Hersteller verwenden.

Für das RAID-Festplattensystem werden die folgenden drei Betriebszustände angezeigt:

- **OK**: Das RAID-Festplattensystem ist in Funktion.

RAID Status
The RAID array status is OK.

- **DEGRADED**: Eine der Festplatten ist defekt und muss ausgetauscht werden. Eine entsprechende Meldung wird auch per E-Mail an den Administrator abgeschickt.

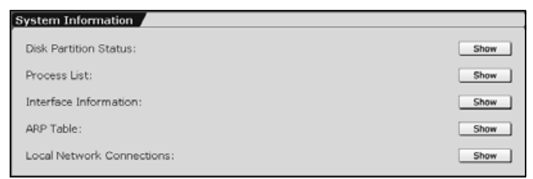
RAID Status
The RAID array is currently DEGRADED, faulty disk is **HDD0 (left harddisk)**.

- **REBUILDING**: Eine neue Festplatte wurde eingebaut und erkannt. Die bestehende Festplatte wird auf die neue Festplatte gespiegelt. Der Vorgang kann 30 Minuten oder länger dauern. Der aktuelle Stand des Speichervorgangs wird in diesem Fenster angezeigt. Vor Beginn und nach Beendigung des Speichervorgangs wird eine entsprechende Notification an den Administrator abgeschickt.

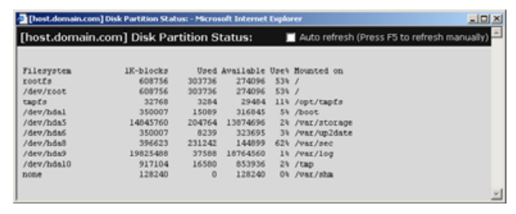


Die Notification Codes sind in Kapitel 5.10.3.2 ab Seite 431 aufgeführt.

System Information

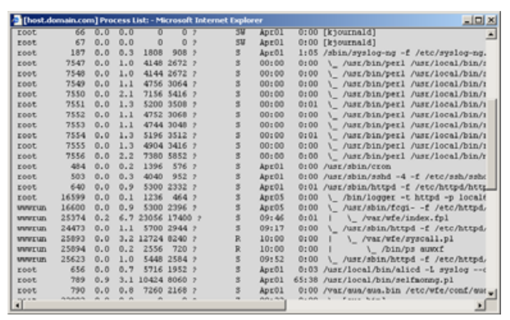


In diesem Menü stehen noch weitere Systeminformationen zur Verfügung. Diese Informationen werden in einem separaten Fenster dargestellt. Durch einen Klick auf die Schaltfläche **Show** werden diese Fenster geöffnet.

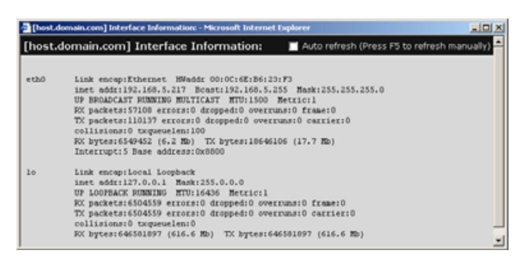


Filesystem	1K-blocks	Used	Available	Use%	Mounted on
rootfs	608756	303736	274096	53%	/
/dev/root	608756	303736	274096	53%	/
tmpfs	32768	3284	29484	11%	/opt/tmpfs
/dev/hda1	350007	15089	316845	5%	/boot
/dev/hda5	14845760	204764	13874696	2%	/var/storage
/dev/hda6	350007	8239	323695	3%	/var/up2date
/dev/hda8	396623	231242	144899	62%	/var/sec
/dev/hda9	19825488	37588	18764560	1%	/var/log
/dev/hda10	917104	16580	853936	2%	/tmp
none	128240	0	128240	0%	/var/shm

Disk Partition: In der Tabelle wird die Partition der Systemdaten und der jeweilige Speicherplatz auf der Festplatte angezeigt.

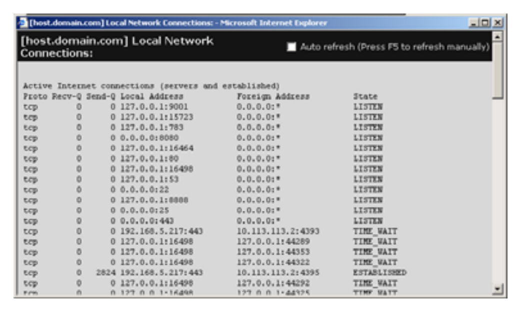


Process List: In der Baumstruktur werden die aktuellen Prozesse auf dem Internet-Sicherheitssystem dargestellt.



Interface Information: In dieser Tabelle werden alle konfigurierten externen und internen Schnittstellen aufgeführt.

ARP Table: Diese Tabelle stellt den ARP-Cache des Systems dar. Dies sind alle dem System bekannten Zuordnungen von IP-Adressen zu Hardware-Adressen (MAC).



Local Network Connections: In der Tabelle werden alle aktuellen Netzwerkverbindung von Ihrem System angezeigt. Verbindungen durch das System werden nicht angezeigt.

5.9. Remote Management (Remote Management)

Im Verzeichnis **Remote Management** befinden sich die Schnittstellen zu weiteren Programmen und Tools, durch die das Sicherheitssystem und die privaten Netzwerke remote verwaltet werden können.

5.9.1. Astaro Command Center (ACC)



In diesem Menü wird der *Device Agent* für das zentrale Management-System **Astaro Command Center** eingeschaltet.

Das *Astaro Command Center* ermöglicht die zentrale Beobachtung und Verwaltung der im Einsatz befindlichen *Astaro-Security-Gateway*-Sicherheitssysteme ab Version 6.1. In der Gesamtübersicht wird für jede der angebundenen Sicherheitssysteme der genaue Status, die aktuelle Version, der aktuelle Stand des Updates, die derzeitige Systemauslastung und die jeweils kritischen Sicherheitsereignisse übersichtlich dargestellt. Der Administrator ist so in der Lage auf Störungen und kritische Ereignisse schnell zu reagieren.

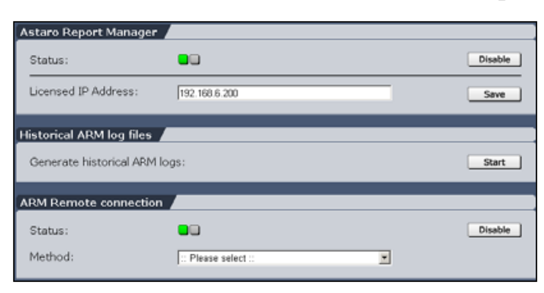
Anbindung an das Astaro Command Center vorbereiten:

Für die Anbindung des Sicherheitssystems an das *Astaro Command Center* muss der **ACC Server** zuvor im Menü **Definitions / Networks** definiert werden. Wählen Sie anschließend im Drop-down-Menü **ACC Server** diesen Server aus. Die Kommunikation zwischen dem Sicherheitssystem *Astaro Security Gateway* und dem *Astaro Command Center* erfolgt über den Port 4433. Der Zugriff auf die Bedienoberfläche des zentralen Management-Systems erfolgt allerdings über das HTTPS-Protokoll auf Port 443.

Nachdem Sie den *ACC-Server* ausgewählt haben wird ein *Fingerprint*

zur zertifizierten Nutzung des installierten *Astaro Command Center* angezeigt. Wenn dieser Fingerprint richtig ist, klicken Sie auf die Schaltfläche **Start**.

5.9.2. Astaro Report Manager (ARM)



Mit dem **Astaro Report Manager** werden die auf den Sicherheitssystemem generierten Log Files gesammelt und ausgewertet. Da die Daten auf dem *Astaro Report Manager* zentral zusammengeführt werden, u. a. auch von Sicherheitslösungen anderer Hersteller, ist der Administrator in der Lage die Meldungen anhand der übersichtlichen Darstellung zu vergleichen, genau zu untersuchen und somit auf Angriffe schnell durch entsprechende Abwehrmaßnahmen zu reagieren. Der *Astaro Report Manager* ist ein eigenständige Produkt und muss separat erworben werden.

Im Menü **ARM** schalten Sie die Schnittstelle zum **Astaro Report Manager (ARM)** ein und führen die Einstellungen zur Erstellung der lokalen Log Files durch: Neben den Einstellungen für die Übermittlung der **ARM Log Files** an den *Astaro Report Manager* können Sie die **ARM Log Files** für das historische Log-File-Archiv generieren und auf einen lokalen Rechner herunterladen.

In diesem Kapitel werden die Funktionen und Einstellungen beschrieben, die im Menü **ARM** enthalten sind. Je nach bestehender Netzwerktopologie und der dafür geplanten Astaro-Report-Manager-Netzwerkarchitektur, müssen für die Integration des Remote Management Tools weitere Einstellungen durchgeführt werden.

Die möglichen Astaro-Report-Manager-Netzwerkarchitekturen sind:

- Lokale ARM-Architektur (Locale ARM Architecture)
- Zentralisierte ARM-Architektur (Centralized ARM Architecture)
- Großangelegte ARM-Architektur (Large-Scale ARM Architecture)

Der Aufbau und die Installation dieser ARM-Netzwerkarchitekturen werden im **ARM/ASG-V6-Integration Guide** beschrieben.



Die Installation der Software und die nötigen Einstellungen zur Anbindung des **Astaro Report Manager** an das Sicherheitssystem **Astaro Security Gateway V6** werden im **ARM/ASG-V6-Integration Guide** beschrieben. Die Nutzung des **Astaro Report Managers** wird in den zugehörigen Handbüchern beschrieben.
Sie finden die aktuellen Handbücher und Guides unter der Internetadresse **http://www.astaro.com/kb**.

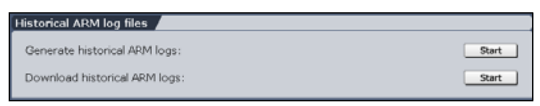
Astaro Report Manager (ARM)

Status: Durch einen Klick auf die Schaltfläche **Enable** schalten Sie die Schnittstelle zum **Astaro Report Manager** und die Funktionen zur Generierung der **ARM Log Files** ein (Statusampel zeigt Grün).

Licensed IP Address: Dieses Eingabefeld wird angezeigt, nachdem Sie die Funktion in der Zeile **Status** eingeschaltet haben.
Der Lizenzumfang des *Astaro Report Manager* hängt von der Anzahl der angebundenen Sicherheitssysteme ab. Diese Sicherheitssysteme werden anhand ihrer IP-Adresse identifiziert. Tragen Sie in das Eingabefeld die IP-Adresse der Netzwerkkarte ein, über die die Log Files an den ARM Syslog Server geschickt werden. Sobald Sie eine gültige IP-Adresse eingegeben haben, werden die *ARM Log Files* während des nächtlichen *Log-File-Rotation*-Prozesses automatisch generiert. Diese Log Files können später über die Funktionen in den anderen Fenstern manuell auf einen lokalen Rechner heruntergeladen oder automatisch

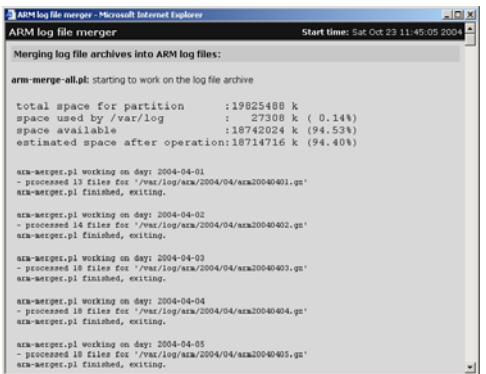
an einen Host geschick werden. Hier gibt es keine Live Logs für die ARM-Protokolle.

Historical ARM Log Files



Mit dieser Funktion generiert das Sicherheitssystem spezielle *Historical Log Files*, die vom *Astaro Report Manager* importiert und ausgewertet werden können.

Generate Historical ARM Logs: Durch einen Klick auf die Schaltfläche **Start** werden alle täglich erzeugten Log Files aus dem Archiv in einem *Historical Log File* zusammengefasst.



Die Generierungsprozess wird im Fenster **ARM Log File Merger** angezeigt. Der Prozess wurde erfolgreich abgeschlossen, wenn in diesem Fenster nur die Meldung **arm-merge-all.pl: finished, exiting** erscheint. Falls der Prozess nicht erfolgreich beendet wurde, erscheint zusätzlich zu der Meldung der Grund des Abbruchs, z. B. **not enough free space availabale, exiting**, falls der Speicherplatz auf der Festplatte nicht ausricht.

Download Historical ARM Logs: Diese Funktion steht zur Verfügung sobald das erste *Historical-Log-File* generiert wurde. Durch einen Klick auf die Schaltfläche **Start** wird ein Dialog geöffnet, mit dem das *ARM Log File* (Datei: **arm_logs.tar**) auf einen lokalen Rechner heruntergeladen werden kann.

ARM Remote Connection

In diesem Fenster konfigurieren Sie den **ARM-Log-Files-Transfer**. Die neuen Einstellungen haben keine Auswirkungen auf bereits bestehende Log Files.

Status: Durch einen Klick auf die Schaltfläche **Enable** schalten Sie die Funktion ein (Statusampel zeigt grün).

Anschließend öffnet sich ein erweitertes Eingabefenster.



Sicherheitshinweis:

Beide Methoden für den Datentransfer sind unverschlüsselt. Wenn die Log Files an einen Server außerhalb des privaten Netzwerks gesendet werden, sollte dies nur durch einen Host-to-Net-IPSec-VPN-Tunnel erfolgen. Eine bestehende Net-to-Net-Verbindung kann nicht verwendet werden!

Method: Für den Datentransfer stehen die Methoden **Syslog** und **SMB/CIFS Share** zur Verfügung. Für beide Methoden müssen Sie auf dem Sicherheitssystem zuerst einen ARM-Server definieren, an den die *ARM Log Files* gesendet werden. Der Server, bzw. Host wird im Menü **Definitions/ Networks** hinzugefügt. Anschließend können Sie die folgenden Einstellungen durchführen:

- Die Methode **Syslog** wird für eine LAN-Netzwerkarchitektur empfohlen. Wenn Sie diese Methode ausgewählt haben, führen Sie die folgenden Einstellungen durch.

  Host: Wählen Sie im Drop-down-Menü den ARM-Server aus, an den die ARM Log Files gesendet werden sollen.

  Service: Stellen Sie in diesem Drop-down-Menü den Dienst ein, der für den Datentransfer verwendet werden soll.



Verwechseln Sie diese Einstellungen nicht mit dem Menü **System/ Remote Syslog**: Dort kann normalerweise nur ein *Syslog-Server* für das Sicherheitssystem definiert werden. Im Menü **ARM** kann der *Astaro Report Manager (ARM)* unabhängig davon als Syslog-Server konfiguriert werden. Damit in diesem Fall der *Astaro Report Manager* reibungslos funktioniert, werden die Daten in einem speziellen ARM-kompatiblen Format übertragen.

- Die Methode **SMB/CIFS Share** wird für eine WAN-Netzwerkarchitektur empfohlen. Wenn Sie diese Methode ausgewählt haben, führen Sie die folgenden Einstellungen durch.

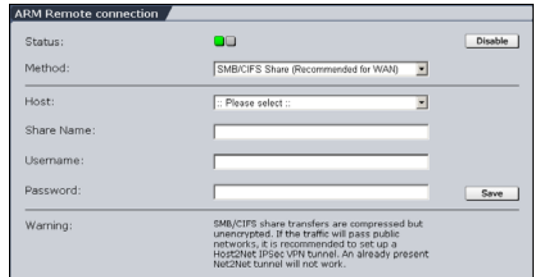
  Host: Wählen Sie im Drop-down-Menü den ARM-Server aus, an den die ARM Log Files gesendet werden sollen.

  Share Name: Tragen Sie in das Eingabefeld den Windows Share Name ein. Stellen Sie sicher, dass im Astaro Report Manager die entsprechenden Rechte für das Verzeichnis definiert wurden.

  Username: Tragen Sie in das Eingabefeld den Benutzernamen für den SMB Account ein.

  Password: Tragen Sie in das Eingabefeld das Passwort für den SMB Account ein.

Speichern Sie die Einstellungen durch einen Klick auf die Schaltfläche **Save**.



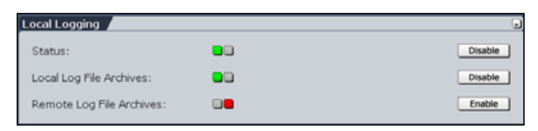
Bei der Übertragung mit der Methode *SMB/CIFS Share* werden die ARM Log Files in einer mit Gzip gepackten ASCII-Datei übermittelt. Die Log Files befinden sich in einem Verzeichnis das nach Jahr und Monat unterteilt ist (**Beispiel**: `arm\2004\10\20041017.gz`).

Die *ARM Log Files* werden generiert, sobald die Schnittstelle zum *Astaro Report Manager* eingeschaltet und im Eingafeld **Licensed IP Address** eine gültige IP-Adresse eingegeben wurde. Nach Konfiguration der Funktion **ARM Remote Connection** werden die *ARM Log Files* an den entsprechenden Server geschickt.

5.10. Local Logs (Log Files)

Im Verzeichnis **Local Logs** werden die vom System generierten Protokolle (Logs) verwaltet.

5.10.1. Settings



Im Fenster **Local Logging** führen Sie die Grundeinstellung für die Log-File-Generierung durch.

Status: Durch einen Klick auf die Schaltfläche **Enable** schalten Sie die Funktion ein (Statusampel zeigt grün).

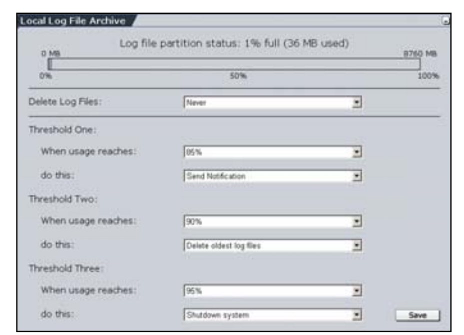
Wichtiger Hinweis:

Wenn die Funktion ausgeschaltet ist, werden vom Internet-Sicherheitssystem keine **Log Files** generiert!

Local Log File Archives: Mit dieser Funktion werden die generierten Log Files lokal auf dem Internet-Sicherheitssystem archiviert. Die Einstellungen für das lokale Log-File-Archiv werden im Fenster **Local Log File Archive** durchgeführt.
Per Default ist die Funktion nach dem Einschalten der Logging-Funktion ebenfalls eingeschaltet.

Remote Log File Archives: Mit dieser Funktion können die generierten Log Files remote auf einem Host oder Server archiviert werden. Die Einstellungen zur Automatisierung der Log-File-Archivierung auf einem separaten Server werden im Fenster **Remote Log File Archive** durchgeführt.

Local Log File Archive



In diesem Fenster können Sie die Auslastung der lokalen Log-File-Partition beobachten. Das Diagramm zeigt den derzeit belegten Speicherplatz in MB sowie die prozentuale Auslastung dieser Partition an.

Im unteren Fenster stellen Sie mit Hilfe der Drop-down-Menüs ein, wie das System reagieren soll, sobald ein bestimmter Anteil der Partition von den Log Files belegt ist. Hierbei können drei Stufen mit jeweils unterschiedlichen Aktionen belegt werden.

Delete Log Files (span of time): Stellen Sie in diesem Drop-down-Menü die Zeitspanne in Tagen ein, nach der die Log Files automatisch vom Sicherheitssystem gelöscht werden.

Log Files Level konfigurieren:

Für jede Stufe können folgende Einstellungen durchgeführt werden:

When Usage reaches: Stellen Sie hier ein, bei welcher prozentualen Auslastung der Partition vom System eine Aktion ausgeführt wird.

do this: Stellen Sie in diesem Auswahlmenü die Aktion ein.

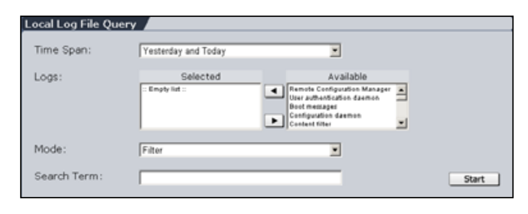
Die verfügbaren Aktionen sind:

- **Delete oldest Log Files**: Die ältesten Log Files werden vom Internet-Sicherheitssystem automatisch gelöscht. Der Administrator erhält zuvor die Notification E-Mail WARN 711.
- **Send Notification**: An den Administrator wird nur die Notification E-Mail INFO 710 mit einer entsprechenden Warnung abgeschickt.
- **Shut down System**: Das Internet-Sicherheitssystem fährt automatisch herunter. Der Administrator erhält zuvor die Notification E-Mail CRIT 712.

- **Nothing**: Es werden keine Aktionen gestartet.

Die Einstellungen übernehmen Sie durch einen Klick auf die Schaltfläche **Save**.

Remote Log File Archive



In diesem Fenster nehmen Sie die Einstellungen für eine ausgelagerte Archivierung der Log Files vor. Falls sich das *Remote Log File Archive* auf einem Server befindet, müssen Sie diesen zuerst im Menü **Definitions/Networks** hinzufügen.

Remote Log File Archive konfigurieren:

1. Schalten Sie im Fenster **Global Settings** die Funktion **Remote Log File Archives** durch einen Klick auf die Schaltfläche **Enable** ein.

   Das Fenster **Remote Log File Archive** wird geöffnet.

2. Wählen Sie im Drop-down-Menü **Type** die Archivierungsart aus.

   Anschließend werden die Drop-down-Menüs und/oder Eingabefelder zur ausgewählten Archivierungsart angezeigt.

3. Führen Sie die Einstellungen für Ihre Archivierungsart durch.

3.1 FTP Server

Host: Wählen Sie im Drop-down-Menü den Host aus.

Port: Wählen Sie im Drop-down-Menü den Port aus.
Per Default ist FTP bereits ausgewählt.

Username: Tragen Sie in das Eingabefeld den Benutzernamen ein.

Passwort: Tragen Sie in das Eingabefeld das Passwort ein.

Remote Path: Tragen Sie in das Eingabefeld den Pfad ein.

3.2 SMB (CIFS) Share

Host: Wählen Sie im Drop-down-Menü den Host aus.

Username: Tragen Sie in das Eingabefeld den Benutzernamen ein.

Passwort: Tragen Sie in das Eingabefeld das Passwort ein.

Share Name: Tragen Sie in das Eingabefeld den Share Name ein.

3.3 Secure Copy (SSH) Server

Public DSA Key: Im Fenster wird der Public DSA Key angezeigt.

Host: Wählen Sie im Drop-down-Menü den Host aus.

Username: Tragen Sie in das Eingabefeld den Benutzernamen ein.

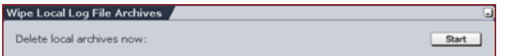
Remote Path: Tragen Sie in das Eingabefeld den absoluten Pfad ein.

3.4 Send by E-Mail

E-Mail Address: Tragen Sie in das Eingabefeld die E-Mail-Adresse ein.

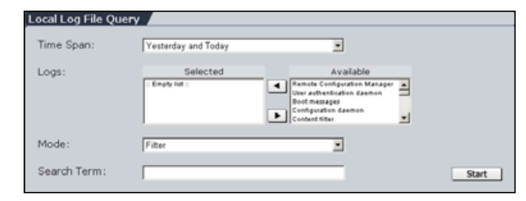
4. Bestätigen Sie Ihre Eingaben durch einen Klick auf die Schaltfläche **Save**.

Wipe Local Log File Archives



Delete local archives now: Das gesamte lokale Log-Archiv mit Ausnahme der aktuellen Protokolle vom heutigen Tag wird gelöscht. Nur durch diese Aktion wird dieses Archiv gelöscht - durch das Ausschalten der Funktion **Local Logging** werden keine Protokolle gelöscht. Der Löschvorgang wird durch einen Klick auf die Schaltfläche **Start** ausgeführt.

5.10.2. Local Log File Query



Mit der Aktion **Local Log File Query** können Sie im lokalen Archiv nach bestimmten **Log Files** suchen. Das Ergebnis der Suchanfrage wird in einem separaten Fenster angezeigt.

Suchanfrage starten:

1. Stellen Sie im Drop-down-Menü **Time Span** die Zeitspanne ein.
2. Wählen Sie im Auswahlfeld **Logs** die Protokolle aus.

   Die Funktionsweise des **Auswahlfeldes** wird in Kapitel 4.3.2 ab Seite 41 beschrieben.
3. Stellen Sie im Drop-down-Menü **Mode** den Modus ein.
4. Falls Sie nach Protokollen mit bestimmten Zeichenketten suchen, tragen Sie diese in das Eingabefeld **Search Term** ein.
5. Um die Suchanfrage zu starten klicken Sie auf die Schaltfläche **Start**.

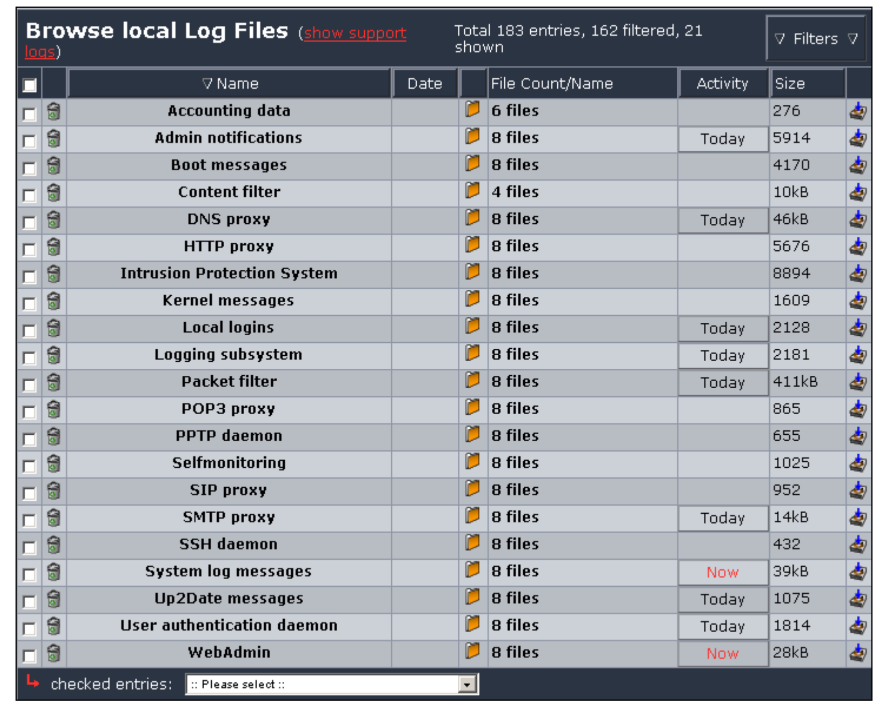
Die Protokolle werden nun in einem separaten Fenster aufgelistet.

5.10.3. Browse

Im Menü **Browse** sind alle Protokolle enthalten. Nach dem Öffnen des Menüs werden in der Übersicht **Browse local Log Files** alle Protokollgruppen (Logs) angezeigt.

Die Log File-Übersicht

In der Übersicht sind alle Protokollgruppen (Log File Groups) enthalten. Die Gruppen mit den heutigen Protokollen können direkt in dieser Übersicht geöffnet werden.



Browse local Log Files (show support logs) Total 183 entries, 162 filtered, 21 shown ▽ Filters ▽

Name	Date	File Count/Name	Activity	Size
Accounting data		6 files		276
Admin notifications		8 files	Today	5914
Boot messages		8 files		4170
Content filter		4 files		10kB
DNS proxy		8 files	Today	46kB
HTTP proxy		8 files		5676
Intrusion Protection System		8 files		8894
Kernel messages		8 files		1609
Local logins		8 files	Today	2128
Logging subsystem		8 files	Today	2181
Packet filter		8 files	Today	411kB
POP3 proxy		8 files		865
PPTP daemon		8 files		655
Selfmonitoring		8 files		1025
SIP proxy		8 files		952
SMTP proxy		8 files	Today	14kB
SSH daemon		8 files		432
System log messages		8 files	Now	39kB
Up2Date messages		8 files	Today	1075
User authentication daemon		8 files	Today	1814
WebAdmin		8 files	Now	28kB

checked entries: :: Please select ::

Die Funktionen in der Übersicht von links nach rechts:

Auswahlkästchen: Diese Einstellung wird in Verbindung mit dem Drop-down-Menü in der Fußzeile der Tabelle benötigt. Markieren Sie hier die Protokollgruppen und wählen Sie anschließend die Aktion

(**Delete** oder **Download as ZIP File**) im Drop-down-Menü aus.
Die Aktion wird sofort gestartet.
Durch einen Klick auf das Auswahlkästchen in der Kopfzeile werden alle Protokollgruppen ausgewählt.

( ): Durch einen Klick auf das Papierkorb-Symbol wird die Gruppe aus der Tabelle gelöscht.

Name: In dieser Spalte sind alle Protokolle alphabetisch aufgelistet.

Date: Das Datum wird bei den heutigen Protokollen nicht angezeigt.

( ): Durch einen Klick auf das Ordner-Symbol wird das Unterverzeichnis mit allen Protokollen dieser Gruppe angezeigt.
Durch einen nochmaligen Klick auf das Symbol gelangen Sie wieder in die Übersicht. Die zusätzlichen Funktionen im Unterverzeichnis werden im Abschnitt „Das Log-File-Unterverzeichnis“ beschrieben.

File Count / Name: In dieser Spalte wird die Anzahl der vorhandenen Dateien (Files) angezeigt. Die alten Protokolle können im Unterverzeichnis geöffnet werden.

Activity: Falls in einer Gruppe seit Mitternacht Prozesse protokolliert werden, wird in dieser Spalte eine entsprechende Meldung angezeigt:

- **Now**: Es werden in diesem Moment Protokolle erstellt.
- **Today**: Es wurden seit Mitternacht Protokolle erzeugt.

Das aktuelle Protokoll (**Live Log**) kann durch einen Klick auf die Meldung **Now** oder **Today** geöffnet werden.

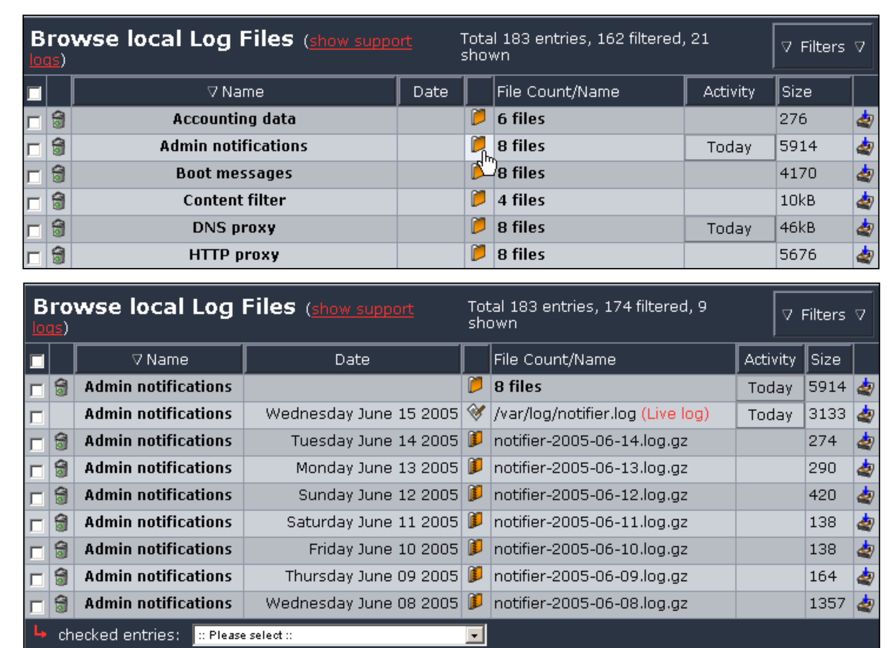
Size: In dieser Spalte wird die Größe der Log-File-Gruppe angezeigt.

( ): Durch einen Klick auf das Download-Symbol können Sie die **Log Files** auf Ihren lokalen Client herunterladen. Diese **Log Files** können anschließend zur Auswertung der Daten in externe Programme z. B. Microsoft Excel importiert werden.

Das Log-File-Unterverzeichnis

Im Unterverzeichnis befinden sich alle Protokolle (Logs) einer Gruppe. Die Untergruppe wird in der Übersicht durch einen Klick auf das Ordner-Symbol () geöffnet.

Die zusätzlichen Funktionen im Unterverzeichnis sind:



Browse local Log Files (show support logs) Total 183 entries, 162 filtered, 21 shown ▽ Filters ▽

		▽ Name	Date		File Count/Name	Activity	Size	
		Accounting data			6 files		276	
		Admin notifications			8 files	Today	5914	
		Boot messages			8 files		4170	
		Content filter			4 files		10kB	
		DNS proxy			8 files	Today	46kB	
		HTTP proxy			8 files		5676	

Browse local Log Files (show support logs) Total 183 entries, 174 filtered, 9 shown ▽ Filters ▽

		▽ Name	Date		File Count/Name	Activity	Size	
		Admin notifications			8 files	Today	5914	
		Admin notifications	Wednesday June 15 2005		/var/log/notifier.log (Live log)	Today	3133	
		Admin notifications	Tuesday June 14 2005		notifier-2005-06-14.log.gz		274	
		Admin notifications	Monday June 13 2005		notifier-2005-06-13.log.gz		290	
		Admin notifications	Sunday June 12 2005		notifier-2005-06-12.log.gz		420	
		Admin notifications	Saturday June 11 2005		notifier-2005-06-11.log.gz		138	
		Admin notifications	Friday June 10 2005		notifier-2005-06-10.log.gz		138	
		Admin notifications	Thursday June 09 2005		notifier-2005-06-09.log.gz		164	
		Admin notifications	Wednesday June 08 2005		notifier-2005-06-08.log.gz		1357	

checked entries: :: Please select ::

Date: Im Unterverzeichnis wird bei den alten Protokollen der Tag und das Datum angezeigt.

(): Durch einen Klick auf das Ordner-Symbol kehren Sie in die Übersicht zurück.

(): Dies ist ein Protokoll von heute. Durch einen Klick auf das Symbol öffnen Sie das **Live-Log**-Fenster.

(): Dies ist ein archiviertes Protokoll. Durch einen Klick auf das Symbol wird das **Log**-Fenster geöffnet.

File Count/Name: Beim heutigen Protokoll wird in dieser Spalte der Pfad zur Log-Datei und die Meldung **Live Log** angezeigt.
Bei den archivierten Log-Dateien steht in dieser Spalte der Dateinamen.

Filters

Mit der Funktion **Filters** können Sie aus der Tabelle *Protokolle* (*Log Files*) mit bestimmten Attributen herausfiltern. Diese Funktion erleichtert das Managen von großen Netzwerken, da Protokolle eines bestimmten Typs übersichtlich dargestellt werden können.

Protokolle filtern:

1. Klicken Sie auf die Schaltfläche **Filters**.

   Anschließend wird das Eingabefenster geöffnet.

2. Tragen Sie in den nachfolgend aufgeführten Feldern die Attribute für den Filter ein. Es müssen nicht alle Attribute definiert werden.

   Group: Falls Sie Protokolle einer bestimmten Gruppe filtern möchten, wählen Sie diese im Drop-down-Menü aus.

   Month: Mit diesem Drop-down-Menü filtern Sie Protokolle aus einem bestimmten Monat.

   Type: Mit diesem Drop-down-Menü filtern Sie Protokolle eines bestimmten Typs.

3. Um den Filter zu starten klicken Sie auf die Schaltfläche **Apply Filters**.

Anscchließend werden nur die gefilterteten Protokolle in der Tabelle angezeigt. Nach Verlassen des Menüs werden wieder alle Protokolle dargestellt.

5.10.3.1. Log-Files

In diesem Kapitel sind alle verfügbaren Protokolle (Logs) aufgeführt. Im Menü **Browse** werden diese Log-Dateien erst angezeigt, wenn vom System entsprechende Prozesse protokolliert wurden. Die nachfolgende Log-Datei **Accounting data** wird z. B. erst angezeigt, nachdem die Funktion **Accounting** im Menü **Network/Accounting** eingeschaltet wurde.

Accounting data: In diesen Log-Dateien sind alle vom System archivierten **Accounting**-Protokolle verfügbar. Im Menü **Reporting/ Accounting** können die Protokolle betrachtet werden.

Admin notifications: In den *Notification*-Log-Dateien werden alle *Notification-E-Mails*, die durch das Internet-Sicherheitssystem abgeschickt wurden, protokolliert. Auf diese Weise kann der Administrator auch kritische Systemvorgänge beobachten, wenn ihn keine *Notification E-Mails* erreicht haben.

Die Fehler-, Warnungs- und Informations-Codes sind in Kapitel 5.10.3.2 ab Seite 431 aufgeführt.

Boot messages: In diesen Log-Dateien werden die Boot-Meldungen protokolliert.

Configuration daemon: In diesen Log-Dateien werden die Aktivitäten des Configuration Daemon protokolliert. Diese Log-Dateien gehören zu den *Support Logs* und werden erst durch einen Klick auf die Schaltfläche **show support logs** angezeigt.

Content filter: In diesen Log-Dateien werden die Aktivitäten der Content Filter zu den Proxies HTTP, SMTP und POP3 protokolliert.

DHCP server: Falls das Internet-Sicherheitssystem als DHCP-Server fungiert und den Clients im Netzwerk dynamische IP-Adressen zuweist, werden die Aktivitäten in diesen Log-Dateien protokolliert.

DNS proxy: In diesen Log-Dateien werden die Aktivitäten des DNS-Proxy protokolliert.

Fallback messages: Diese Log-Dateien dienen als Sicherheitsarchiv für protokollierte Prozesse, die keinem der Log-Dateien zugeordnet werden können. Diese Log-Dateien gehören zu den Support Logs und werden erst durch einen Klick auf die Schaltfläche **show support logs** angezeigt. In der Regel sind diese Log-Dateien leer.

High availability: In diesen Log-Dateien werden die Aktivitäten des *High-Availability-(HA)*-Systems protokolliert.

HTTP accessed sites: In diesen Log-Dateien werden die angeforderten Internetseiten protokolliert.

HTTP blocked sites: In diesen Log-Dateien werden alle vom *Content Filter* geblockten Internetseiten protokolliert.

HTTP daemon: Die Log-Dateien zum HTTP Daemon gehören zu den Support Logs und werden erst durch einen Klick auf die Schaltfläche **show support logs** angezeigt.

HTTP proxy: In den *HTTP Proxy Logs* werden die Aktivitäten von *HTTP Clients* protokolliert.

Ident proxy: In diesen Log-Dateien werden die Aktivitäten des Ident-Proxy protokolliert.

Intrusion Protection System: In diesen Log-Dateien werden die Aktivitäten des *Intrusion Protection System (IPS)* protokolliert.

IPSec VPN: In diesen Log-Dateien werden umfangreiche Informationen zu den Einstellungen der *IPSec-VPN-* und *L2TP-over-IPSec-*Verbindungen protokolliert. Dies beinhaltet auch Informationen zum Schlüsselaustausch (Key Exchange) und zur Verschlüsselung (Encryption).

Kernel messages: In den **Kernel**-Logs wird der System-Status protokolliert, inklusive der Meldungen von den Gerätetreibern, der Meldung des Boot-Prozesses sowie der vom Paketfilter (Packet Filter) geblockten Datenpakete.

License information: In diesen Log-Dateien werden die Statusinformationen des License Daemon *alicd* protokolliert. Diese Log-Dateien gehören zu den *Support Logs* und werden erst durch einen Klick auf die Schaltfläche **show support logs** angezeigt.

Logging subsystem: In diesen Log-Dateien werden z. B. Vorgänge zur lokalen Archivierung der Log-Dateien auf dem Sicherheitssystem, zu versendeten Dateien an das *Remote-Log-File*-Archive und zu abgesendeten Notifications protokolliert.

Local logins: In diesen Log-Dateien werden Informationen zu Einlogg-Prozessen in die lokale Konsole protokolliert.

MiddleWare: In diesen Log-Dateien werden die Aktivitäten in der MiddleWare protokolliert. Diese Log-Dateien gehören zu den Support Logs und werden erst durch einen Klick auf die Schaltfläche **show support logs** angezeigt.

Network accounting daemon: In diesen Log-Dateien wird die Funktionsfähigkeit des Accounting protokolliert.

Packet filter: In den *Packet Filter* Logs werden alle geblockten Datenpakete protokolliert. Diese Log Files sind ein Teil der Kernel-Logs.

POP3 proxy: In diesen Log-Dateien werden die Aktivitäten des POP3-Proxy protokolliert. Alle ausgehenden E-Mails werden darin aufgeführt. Zusätzlich werden alle Unregelmäßigkeiten, z. B. Ausfälle oder blockierte E-Mails protokolliert.

Portscan: Die Funktion *Portscan Detection* erkennt Portscans und benachrichtigt den Administrator per E-Mail. Wenn Sie die **Log Files** in diesem Menü analysieren, ziehen Sie keine voreiligen Schlüsse hinsichtlich der in diesen Protokollen angegebenen Quelladresse (SRC - IP Source Address) und dem Quell-Port (SPT – Source Port). Diese Angaben können vom eigentlichen Absender leicht gefälscht werden. Nützliche Informationen erhält man durch die Auswertung der Ziel-Adresse (DST – Destination IP Adresses) und des Ziel-Portes (DPT – Destination Port).

PPP daemon: Diese Log-Dateien werden generiert, wenn *Modem dialup* konfiguriert wurde. In den Log-Dateien werden Aktivitäten vom PPP Daemon und vom *chat*-Programm protokolliert. Das *chat*-Programm handelt Details bei den PPP-Verbindungen aus.

PPPoA: In diesen Log-Dateien werden die Vorgänge bei der Einwahl mit *PPP over ATM* protokolliert.

PPPoE: In diesen Log-Dateien werden die Vorgänge bei der Einwahl mit *PPP over Ethernet* protokolliert.

PPTP daemon: In den PPTP-Logs wird der Verlauf beim Zugriff des externen Clients auf das System protokolliert. Dies beinhaltet das Einloggen und die Authentifizierung sowie eventuelle Fehler beim Verbindungsaufbau.

Wenn Sie im Menü **Network/PPTP VPN Access** für die Funktion **Logging** den Parameter **Extensive** eingestellt haben, werden im PPTP-Log auch ausführliche Informationen zur PPP-Verbindung angezeigt.

Remote Configuration Manager: Wenn das Internet-Sicherheitssystem remote über den *Astaro Configuration Manager* konfiguriert wird, werden die entsprechenden Vorgänge in diesen Log Files protokolliert.

Selfmonitoring: Das **Selfmonitoring** gewährleistet die Systemintegrität des Sicherheitssystems und setzt den Administrator über wichtige Ereignisse in Kenntnis. Das Selfmonitoring überwacht die Funktion, Performance und Sicherheit der relevanten System-Parameter und greift bei Abweichungen, die über eine gewisse Toleranz hinausgehen, regulierend ein. Anschließend erhält der zuständige Administrator per E-Mail einen Bericht.

Das **Selfmonitoring** des Internet-Sicherheitssystems stellt sicher, dass zentrale Dienste z. B. der Syslog Daemon, der HTTP-Proxy oder das Network-Accounting ordnungsgemäß funktionieren.

Zugriffsrechte auf Dateien werden ebenso überwacht wie der Anteil einzelner Prozesse am Verbrauch der Systemresourcen, wodurch eine

eventuelle Überlastung des Systems bereits im Vorfeld verhindert wird. Darüber hinaus erhält der Systemverwalter rechtzeitig Hinweise auf sich abzeichnende Ressourcen-Engpässe, wenn z. B. der verfügbare Festplattenspeicher knapp werden sollte. Erforderliche Maßnahmen zur Systemerweiterung bzw. Entlastung können so rechtzeitig geplant werden.

SIP proxy: In diesen Log-Dateien werden die Aktivitäten des SIP-Proxy protokolliert.

SMTP proxy: In diesen Log-Dateien werden die Aktivitäten des SMTP-Proxy protokolliert. Alle eingehenden E-Mails werden darin aufgeführt. Zusätzlich werden alle Unregelmäßigkeiten, z. B. zugewiesene **Bounce**-Stati, Ausfälle oder blockierte E-Mails protokolliert.

SOCKS proxy: In diesen Log-Dateien werden die Aktivitäten des SOCKS-Proxy protokolliert.

SSH daemon: In diesen Log-Dateien werden Informationen zu Einlogg-Prozessen in die Remote Shell protokolliert.

System log messages: In diesen generischen *Log*-Dateien werden verschiedene Informationen zu Daemon-Prozessen auf dem Internet-Sicherheitssystem protokolliert. In diesen Log-Dateien werden unter anderem der Zugriff auf den **SNMP**-Dienst und die Aktivitäten der Funktion **Dynamic DNS** protokolliert.

Up2Date messages: In diesen Log-Dateien werden die Aktivitäten des Moduls **Up2Date Service** protokolliert. Dies beinhaltet die *System*- und die *Pattern-Up2Date*-Prozesse.

Uplink Failover daemon: In diesen Log-Dateien werden die Aktivitäten der konfigurierten Ausfallsicherungen Auf den Netzwerkkarten protokolliert.

User authentication daemon: In diesen Log-Dateien werden die Aktivitäten des AUA Daemon protokolliert. AUA wird für diverse Dienste als zentraler Authentifizierungs-Daemon eingesetzt.

WebAdmin: In diesen Log-Dateien wird die Nutzung des Konfigurationstools *WebAdmin* protokolliert. Die Protokolle beinhalten die über das Konfigurationstool durchgeführten Einstellungsänderungen sowie die Ein- und Auslog-Prozesse.

5.10.3.2. Notification Codes

Hier sind alle Fehler-, Warnungs- und Informations-Codes aufgeführt:

INFO:

000 System was restarted

Das System wurde neu gestartet (gebootet).

010 Configuration Auto Backup

Eine Backup-Datei wurde vom System automatisch generiert und per E-Mail an den Administrator verschickt.

020 License expiry: A feature will expire

Das Abo für eine Sicherheitsanwendung läuft in kürze ab. Weitere Informationen sind in der Notification-E-Mail enthalten.

021 License expiry: A feature expires today!

Das Abo für eine Sicherheitsanwendung läuft heute ab. Weitere Informationen sind in der Notification-E-Mail enthalten.

022 License expiry: A feature is expired!

Das Abo für eine Sicherheitsanwendung ist abgelaufen. Weitere Informationen sind in der Notification-E-Mail enthalten.

025	License usage: Above 80% of User Count on Astaro Security Gateway Lizenznutzung: Die Anzahl der Benutzer ist bei dieser Lizenz begrenzt. Zum aktuellen Zeitpunkt sind mehr als 80% der verfügbaren IP-Adressen vergeben. Die Angaben zu Ihrer Lizenz finden Sie im Menü System/Licensing. Die Benutzer werden anhand ihrer IP-Adresse im Fenster Licensed Users aufgelistet.
040	Remote Configuration Manager – system information
050	UPS device connected Ein UPS-Gerät wurde angeschlossen und vom Sicherheitssystem erkannt.
051	UPS device disconnected Das UPS-Gerät wurde vom USB Port getrennt.
053	UPS power restored Die Spannungsversorgung des UPS-Geräts ist wiederhergestellt.
062	RAID rebuild process started Die RAID-Festplatte wird nun wiederhergestellt. Der aktuelle Stand des Vorgangs wird im Menü Reporting/Advanced angezeigt.
063	RAID rebuild process finished Der Vorgang zur Wiederherstellung der RAID-Festplatte ist abgeschlossen. Ihr RAID-Festplattensystem ist wieder in Funktion.

080	HA check: Version conflict. Trying System Up2Date Eine HA-Überprüfung wurde durchgeführt. Es wurde festgestellt, dass die Versionen der beiden Sicherheitssysteme nicht übereinstimmen. Ein System-Up2Date-Versuch wird gestartet. Beachten Sie bei der Installation des High-Availability-Systems die Hinweise in Kapitel 5.1.11 ab Seite 122.
081	HA check: /opt/tmpfs/config-backup.md5.old does not exist Eine HA-Überprüfung wurde durchgeführt. Es wurde festgestellt, dass die zuvor genannnte Datei nicht vorhanden ist.
082	HA check: /opt/tmpfs/config-backup.md5.new does not exist Eine HA-Überprüfung wurde durchgeführt. Es wurde festgestellt, dass die zuvor genannnte Datei nicht vorhanden ist.
083	HA check: /opt/tmpfs/config-backup.tar does not exist Eine HA-Überprüfung wurde durchgeführt. Es wurde festgestellt, dass die zuvor genannnte Datei nicht vorhanden ist.
084	HA check: /etc/wfe/conf/ does not exist Eine HA-Überprüfung wurde durchgeführt. Es wurde festgestellt, dass das zuvor genannte Verzeichnis nicht vorhanden ist.

085 HA check: opt/tmpfs/config-backup.tar.3des or /etc/ha/des-keyfile does not exist

Eine HA-Überprüfung wurde durchgeführt. Es wurde festgestellt, dass eine der zuvor genannnten Dateien nicht vorhanden ist.

086 HA check: synced config-backupfile md5sum does not match signature

Eine HA-Überprüfung wurde durchgeführt. Die MD5-Prüfsumme der synchronisierten Config-Backup-Datei passt nicht zur Signatur.

087 HA check: Slave is running, HA system is active and working

Das System 2 im Hot-Standby-Modus ist in Betrieb, das HA-System ist aktiv.

105 Astaro User Authenticator (AUA) not running – restarted

Das Programm Astaro User Authenticator (AUA) wird nicht ausgeführt – ein Restart wurde durchgeführt.

106 Cron Task Scheduler not running – restarted

Das Programm Cron Task Scheduler wird nicht ausgeführt – ein Restart wurde durchgeführt.

107 WebAdmin webserver not running – restarted

Der WebAdmin-Webserver wird nicht ausgeführt – ein Restart wurde durchgeführt.

108 ssh server not running – restarted

Der SSH-Server wird nicht ausgeführt – ein Restart wurde durchgeführt.

109	license server not running – restarted Der License-Server wird nicht ausgeführt – ein Restart wurde durchgeführt.
110	configuration database server not running – restarted Der Configuration-Database-Server wird nicht ausgeführt – ein Restart wurde durchgeführt.
111	syslog server not running – restarted Der Syslog-Server wird nicht ausgeführt – ein Restart wurde durchgeführt.
112	middleware not running – restarted Die MiddleWare wird nicht ausgeführt – ein Restart wurde durchgeführt.
113	alicd not running – restarted alicd wird nicht ausgeführt – ein Restart wurde durchgeführt.
114	ulogd not running – restarted ulogd wird nicht ausgeführt – ein Restart wurde durchgeführt.
115	snort not running – restarted snort wird nicht ausgeführt – ein Restart wurde durchgeführt.
116	snmpd daemon not running – restarted Der snmpd Daemon wird nicht ausgeführt – ein Restart wurde durchgeführt.
117	pop3 daemon not running – restarted Der pop3 Daemon wird nicht ausgeführt – ein Restart wurde durchgeführt.

118	hyperdyper daemon not running – restarted Der hyperdyper Daemon wird nicht ausgeführt – ein Restart wurde durchgeführt.
119	named not running – restarted named wird nicht ausgeführt – ein Restart wurde durchgeführt.
120	sockd not running – restarted sockd wird nicht ausgeführt – ein Restart wurde durchgeführt.
121	identd not running – restarted identd wird nicht ausgeführt – ein Restart wurde durchgeführt.
122	dhcpd not running – restarted dhcpd wird nicht ausgeführt – ein Restart wurde durchgeführt.
123	nacctp not running – restarted nacctp wird nicht ausgeführt – ein Restart wurde durchgeführt.
124	ufod not running – restarted ufod wird nicht ausgeführt – ein Restart wurde durchgeführt.
125	smtpd not running – restarted smtpd wird nicht ausgeführt – ein Restart wurde durchgeführt.
126	dyndns not running – restarted dyndns wird nicht ausgeführt – ein Restart wurde durchgeführt.

127	spamd not running – restarted spamd wird nicht ausgeführt – ein Restart wurde durchgeführt.
128	pptpd not running – restarted pptpd wird nicht ausgeführt – ein Restart wurde durchgeführt.
129	httpd-loopback not running – restarted httpd-loopback wird nicht ausgeführt – ein Restart wurde durchgeführt.
130	winbindd not running – restarted winbindd wird nicht ausgeführt – ein Restart wurde durchgeführt.
131	xinetd not running – restarted xinetd wird nicht ausgeführt – ein Restart wurde durchgeführt.
132	virus scanner aveserver not running – restarted virus scanner aveserver wird nicht ausgeführt – ein Restart wurde durchgeführt.
133	squid not running – restarted squid wird nicht ausgeführt – ein Restart wurde durchgeführt.
134	ipsec starter not running – restarted ipsec starter wird nicht ausgeführt – ein Restart wurde durchgeführt.
135	ipsec pluto not running – restarted ipsec pluto wird nicht ausgeführt – ein Restart wurde durchgeführt.

136	device agent not running – restarted device agent wird nicht ausgeführt – ein Restart wurde durchgeführt.
137	virus scanner clamd not running – restarted virus scanner clamd wird nicht ausgeführt – ein Restart wurde durchgeführt.
138	spam release http daemon not running – restarted spam release http daemon wird nicht ausgeführt – ein Restart wurde durchgeführt.
150	Root partition mounted at / is filling up - please check Die Root-Partition im Verzeichnis /.. füllt sich.
151	tmpfs partition mounted at /opt/tmpfs is filling up - please check Die tmpfs-Partition im Verzeichnis /opt/tmpfs füllt sich.
152	secure application partition mounted at /var/sec is filling up - please check Die Secure-Application-Partition im Verzeichnis /var/sec füllt sich.
153	logfile partition mounted at /var/log is filling up - please check Die Log-File-Partition im Verzeichnis /var/log füllt sich.
154	storage application partition mounted at /var/storage is filling up - please check Die Storage-Application-Partition im Verzeichnis /var/storage füllt sich.

155	Up2Date partition mounted at /var/up2date is filling up - please check Die Up2Date-Partition im Verzeichnis /var/up2-date füllt sich.
161	tmpfs partition mounted at /opt/tmpfs is short of inodes - please check Die tmpfs-Partition im Verzeichnis /opt/tmpfs wird knapp – bitte prüfen.
162	secure application partition mounted at /var/sec is short of inodes - please check Die Secure-Application-Partition im Verzeichnis /var/sec wird knapp – bitte prüfen.
163	logfile partition mounted at /var/log is short of inodes - please check Die logfile-Partition im Verzeichnis /var/log wird knapp – bitte prüfen.
164	storage application partition mounted at /var/storage is short of inodes - please check Die Storage-Application-Partition im Verzeichnis /var/storage wird knapp – bitte prüfen.
165	Ud2Date partition mounted at /var/up2date is short of inodes - please check Die Up2Date-Partition im Verzeichnis /var/up2date wird knapp – bitte prüfen.
166	tmp partition mounted at /temp is short of inodes - please check Die temp-Partition im Verzeichnis /tmp wird knapp – bitte prüfen.

169	tmp partition mounted at /tmp is filling up - please check Die tmp-Partition im Verzeichnis /tmp füllt sich.
170	alicd not writing periodic dump file - please check alicd protokolliert keinen zyklischen Speicherauszug mehr – bitte prüfen.
171	hyperdyper daemon not working – restarted Der Hyperdyper Daemon wird nicht ausgeführt – ein Restart wurde durchgeführt.
300	System Up2Date: System Up2Date started System Up2Date wurde gestartet. Weitere Informationen zu System Up2Date erhalten Sie in Kapitel 5.1.3 ab Seite 60.
301	System Up2Date failed: Authentication error. Trying another Authentication Server. Der System Up2Date ist fehlgeschlagen. Während der Authentisierung ist ein Fehler aufgetreten. Der Versuch wird über einen anderen Authentisierungs-Server wiederholt.
302	System Up2Date: No new System Up2Date Packages available Es sind keine neuen System-Up2Date-Pakete verfügbar. Ihr Internet-Sicherheitssystem ist auf dem neusten Stand.
303	System Up2Date succeeded: Prefetched new System Up2Date package(s) Ein oder mehrere neue System-Up2Date-Pakete wurden erfolgreich auf dem Internet-Sicherheits-

system eingespielt. Weitere Informationen zum neuen Up2Date-Paket erhalten Sie in der Notification-E-Mail.
Weitere Informationen zu System Up2Date erhalten Sie in Kapitel 5.1.3 ab Seite 60.

320	System Up2Date failed: Invalid License
	Der System Up2Date ist fehlgeschlagen. Sie haben keine entsprechend gültige Lizenz.
321	System Up2Date: Started in HA-Master mode
	Auf dem Internet-Sicherheitssystem im Normal-Modus (Master) des High-Avialability-Systems wurde der System Up2Date gestartet.
322	System Up2Date: New System Up2Dates installed
	Ein oder mehrere System-Up2Date-Pakete wurden erfolgreich auf dem Internet-Sicherheitssystem installiert. Weitere Informationen erhalten Sie in der Notification-E-Mail.
323	System Up2Date: Started System Up2Date Installer
	Die Installation eines oder mehrerer System-Up2Date-Pakete wurde gestartet.
354	Pattern Up2Date succeeded: Updated new Intrusion Protection patterns
	Ein oder mehrere neue Pattern-Up2Date-Pakete wurden für das Modul Intrusion Protection erfolgreich auf dem Internet-Sicherheitssystem installiert. Weitere Informationen erhalten Sie in der Notification-E-Mail. Weitere Informationen zu System Up2Date erhalten Sie in Kapitel 5.1.3 ab Seite 60.

361	Pattern Up2Date succeeded: Virus Protection Pattern Up2Date installed Ein oder mehrere neue Pattern-Up2Date-Pakete für Virus Protection wurden erfolgreich auf dem Internet-Sicherheitssystem installiert. Weitere Informationen zum neuen Up2Date-Paket erhalten Sie in der Notification-E-Mail.
362	Pattern Up2Date succeeded: Spam Protection Pattern Up2Date installed Ein oder mehrere neue Pattern-Up2Date-Pakete für Spam Protection wurden erfolgreich auf dem Internet-Sicherheitssystem installiert. Weitere Informationen zum neuen Up2Date-Paket erhalten Sie in der Notification-E-Mail.
700	Daily log file archive Dies ist eine Archiv-Datei. Das Datum dieser Log Files wird in der Notification angegeben.
710	Log file partition is filling up Die Log-File-Partition füllt sich. Die derzeit erreichte Auslastung der Partition wird in der Notification angezeigt. Die Aktion des Internet-Sicherheitssystems richtet sich nach den Einstellungen im Menü Local Logs/Settings. Prüfen Sie die Einstellungen im WebAdmin und löschen Sie zur Sicherheit manuell alte Log-Dateien, damit vom Internet-Sicherheitssystem keine wichtigen Log Files entfernt werden. Die gelöschten Dateien und/oder Verzeichnisse werden im Anhang aufgelistet.

720 Executive report

Die Notification enthält den heutigen Executive Report. Weitere Informationen zum Executive Report erhalten Sie in Kapitel 5.8.12 ab Seite 404.

850 Intrusion Protection Alert

Es wurde ein Paket entdeckt, das evtl. Teil eines Intrusion-Versuchs sein kann. Die Regel hat diesen Angriff als niedrige Priorität eingestuft und das Datenpaket wurde nicht abgefangen. Falls diese Pakete in Zukunft abgefangen werden sollen, stellen Sie im WebAdmin bei der entsprechenden Intrusion-Protection-Regel die Aktion „Drop“ ein. Beachten Sie dabei, dass dann eventuell auch regulärer Datenverkehr abgefangen werden kann. Weitere Informationen erhalten Sie in der Notification E-Mail.

851 Intrusion Protection Alert – Event buffering activated

Es wurde ein Paket entdeckt, das evtl. Teil eines Intrusion-Versuchs sein kann. Die Regel hat diesen Angriff als niedrige Priorität eingestuft das Datenpaket wurde nicht abgefangen. Der Ereignispuffer wurde aktiviert. Weitere Intrusion-Protection-Ereignisse werden gesammelt und an Sie abgesendet, sobald die Sammelperiode abgeschlossen ist. Wenn weitere Ereignisse auftreten, wird diese Periode ausgedehnt. Falls diese Pakete in Zukunft abgefangen werden sollen, stellen Sie im WebAdmin bei der entsprechenden Intrusion-Protection-Regel die Aktion „drop“ ein. Beachten Sie dabei, dass dann auch

	eventuell regulärer Datenverkehr abgefangen werden kann. Weitere Informationen erhalten Sie in der Notification E-Mail.
852	Intrusion Protection Alert
	Es wurde ein Paket entdeckt, das evtl. Teil eines Intrusion-Versuchs sein kann. Die Regel hat das Datenpaket automatisch abgefangen. Bei dieser Intrusion-Protection-Regel kann im WebAdmin zwischen den Aktionen „Alert only (nur alarmieren)“ und „Drop (abfangen)“ umgeschaltet werden. Weitere Informationen erhalten Sie in der Notification E-Mail.
853	Intrusion Protection Alert – Event buffering activated
	Es wurde ein Paket entdeckt, das evtl. Teil eines Intrusion-Versuchs sein kann. Die Regel hat das Datenpaket automatisch abgefangen. Der Ereignispuffer wurde aktiviert. Weitere Intrusion-Protection-Ereignisse werden gesammelt und an Sie abgesendet, sobald die Sammelperiode abgeschlossen ist. Wenn weitere Ereignisse auftreten, wird diese Periode ausgedehnt. Bei dieser Intrusion-Protection-Regel kann im WebAdmin zwischen den Aktionen „Alert only (nur alarmieren)“ und „Drop (abfangen)“ umgeschaltet werden. Weitere Informationen erhalten Sie in der Notification E-Mail.
999	File transfer request
	Dies ist die Datei, die Sie angefragt haben.

WARN:

005 Failed login

Ein Versuch sich in das Internet-Sicherheitssystem einzuloggen ist fehlgeschlagen. In der Notification wird die IP-Adresse, die Uhrzeit und der Benutzernamen des betreffenden Benutzers angezeigt.

025 License usage: Exceeding 90% of user count on Astaro Security Gateway

Lizenznutzung: Die Anzahl der möglichen Benutzer liegt zur Zeit bei 90%.

030 Primary Internet uplink is down, switching to backup line

Die primäre Verbindung (Primary Interface) zum Internet ist ausgefallen. Der Uplink erfolgt nun über den Ersatzinternetzugang.

031 Primary Internet uplink is up again, switching back to main line

Die primäre Verbindung (Primary Interface) zum Internet ist wieder aktiv. Der Uplink erfolgt wieder über die primäre Verbindung.

052 UPS on battery power

Das UPS-Gerät läuft im Batteriebetrieb.

061 RAID degraded: defective hard disk inserted

Die Festplatte .... ist defekt. Es ist nicht ratsam das RAID-Festplattensystem im aktuellen Zustand weiter zu betreiben. Das RAID-System wird nicht automatisch wiederhergestellt. Falls der Betrieb mit der defekten Festplatte fort-

gesetzt werden soll, ist ein Neustart des Sicherheitssystems notwendig.

080 HA check: no link beat on interface – retrying

Die Überwachung des Firewall-Systems im Normal-Modus mittels Link Beat ist fehlgeschlagen. Der Versuch wird neu gestartet. Falls die Funktionen nach mehreren Versuchen nicht gestartet werden kann, erhält der Administrator die Notification-E-Mail WAR 081.
Falls Sie für das HA-System diese Überwachungsfunktion nicht einsetzen, müssen Sie keine weiteren Schritte einleiten. Nachdem vom Internet-Sicherheitssystem die Nachricht WAR 081 verschickt wurde, erfolgt kein weiterer Versuch mehr, die Überwachung mittels Link Beat zu starten.

081 HA check: interface does not support link beat check

Die Funktion zur Überwachung des Firewall-Systems im Normal-Modus mittels Link Beat konnte trotz mehrer Versuche nicht gestartet werden. Falls es sich hierbei um eine Neuinstallation des HA-Systems handelt und Sie die Überwachung mittels Link Beat beabsichtigen, vergewissern Sie sich bitte, dass die Netzwerkkarten vom Internet-Sicherheitssystem unterstützt werden. Des Weiteren prüfen Sie bitte auf beiden Firewall-Systemen ob für die Datentransfer-Verbindung die link-beat-fähige Netzwerkkarte ausgewählt wurde.
Die Installation und die Funktionsweise des HA-

Systems wird in Kapitel 5.1.11 ab Seite 122 erklärt.

082	HA check: Error with rsync for System Up2Date Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
083	HA check: Error with rsync for Pattern Up2Date Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
084	HA check: Error with rsync for Intrusion Protection Pattern Up2Date Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
085	HA check: Version conflict between master and slave machine detected Beachten Sie bei der Installation des High-Availability-Systems die Hinweise in Kapitel 5.1.11 ab Seite 122. Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
086	HA check: No Slave contact, please check your HA system Das System 1 (Normal-Modus) erhält vom System 2 (Hot-Stand-by-Modus) keine Rückmeldung mehr. Bitte prüfen Sie das HA-System.

103	Too much swap usage!
156	Version Conflict. Master version lower than slave version. Rebooting system Beachten Sie bei der Installation des High-Availability-Systems die Hinweise in Kapitel 5.1.11 ab Seite 122. Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
157	Version Conflict. Master version lower than slave version. Updating Slave ... Beachten Sie bei der Installation des High-Availability-Systems die Hinweise in Kapitel 5.1.11 ab Seite 122. Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
158	Interface uplink usage exceeds configured limit Auf einer Standard-Ethernet-Schnittstelle wurde die Funktion „Monitor Interface Usage“ eingeschaltet. Der maximale Wert für die Uplink-Bandbreite wurde überschritten.
159	Interface downlink usage exceeds configured limit Auf einer Standard-Ethernet-Schnittstelle wurde die Funktion „Monitor Interface Usage“ eingeschaltet. Der maximale Wert für die Downlink-Bandbreite wurde überschritten.

160	Root partition mounted at / is short of inodes – please check Die Root-Partition im Verzeichnis ... wird knapp – bitte prüfen.
711	Log file(s) have been deleted Die derzeit erreichte Auslastung der Partition wird in der Notification angezeigt. Log-Dateien wurden gelöscht. Prüfen Sie die Einstellungen im WebAdmin und löschen Sie zur Sicherheit manuell alte Log-Dateien, damit vom Internet-Sicherheitssystem keine weiteren wichtigen Log Files entfernt werden. Die gelöschten Dateien und/oder Verzeichnisse werden im Anhang aufgelistet.
715	Remote log file storage failed Das tägliche Log-File-Archiv kann nicht auf dem konfigurierten Remote Server gespeichert werden. Bitte prüfen Sie die Einstellungen im Menü: Local Logs/Settings/Remote log file archive Die Archivdatei wird automatisch mit dem nächsten täglichen Log-File-Archiv abgeschickt.
850	Intrusion Protection Alert Es wurde ein Paket entdeckt, das evtl. Teil eines Intrusion-Versuchs sein kann. Die Regel hat diesen Angriff als mittlere Priorität eingestuft. Weitere Informationen erhalten Sie in der Notification E-Mail.
851	Intrusion Protection Alert – Event buffering activated Es wurde ein Paket entdeckt, das evtl. Teil eines Intrusion-Versuchs sein kann. Die Regel

hat diesen Angriff als mittlere Priorität eingestuft. Der Ereignispuffer wurde aktiviert. Weitere Intrusion-Protection-Ereignisse werden gesammelt und an Sie abgesendet, sobald die Sammelperiode abgeschlossen ist. Wenn weitere Ereignisse auftreten, wird diese Periode ausgedehnt. Weitere Informationen erhalten Sie in der Notification E-Mail.

852 Intrusion Protection Alert

Es wurde ein Paket entdeckt, das evtl. Teil eines Intrusion-Versuchs sein kann. Die Regel hat diesen Angriff als mittlere Priorität eingestuft und hat das Datenpaket automatisch abgefangen. Bei dieser Intrusion-Protection-Regel kann im WebAdmin zwischen den Aktionen „Alert only (nur alarmieren)“ und „Drop (abfangen)“ umgeschaltet werden. Weitere Informationen erhalten Sie in der Notification E-Mail.

853 Intrusion Protection Alert – Event buffering activated

Es wurde ein Paket entdeckt, das evtl. Teil eines Intrusion-Versuchs sein kann. Die Regel hat diesen Angriff als mittlere Priorität eingestuft und hat das Datenpaket automatisch abgefangen. Der Ereignispuffer wurde aktiviert. Weitere Intrusion-Protection-Ereignisse werden gesammelt und an Sie abgesendet, sobald die Sammelperiode abgeschlossen ist. Wenn weitere Ereignisse auftreten, wird diese Periode ausgedehnt. Bei dieser Intrusion-Protection-Regel kann im WebAdmin zwischen den Aktionen „Alert only (nur alarmieren)“ und „Drop (abfangen)“ um-

geschaltet werden. Weitere Informationen erhalten Sie in der Notification E-Mail.

854	Anomaly Intrusion Protection Alert Es wurde ein Paket entdeckt, das evtl. Teil eines Intrusion-Versuchs sein kann. Der Alarm wurde vom Modul Anomaly Detection generiert. Das Paket wurde “nicht” abgefangen. Es gibt mehrere Möglichkeiten, wodurch ein Paket als “ungewöhnlich” eingestuft werden kann. Beim Modul Anomaly Detection erfolgt dies aufgrund von statistischen Daten die durch Überwachung des normalen Datenverkehrs gesammelt werden – Netzwerkpakete mit ungewöhnlichen Eigenschaften werden dann protokolliert.
855	Anomaly Intrusion Protection Alert – Event buffering activated Es wurde ein Paket entdeckt, das evtl. Teil eines Intrusion-Versuchs sein kann. Der Alarm wurde vom Modul Anomaly Detection generiert. Das Paket wurde “nicht” abgefangen. Der Ereignispuffer wurde aktiviert. Weitere Intrusion-Protection-Ereignisse werden gesammelt und an Sie abgesendet, sobald die Sammelperiode abgeschlossen ist. Wenn weitere Ereignisse auftreten, wird diese Periode ausgedehnt. Weitere Informationen erhalten Sie in der Notification E-Mail. Es gibt mehrere Möglichkeiten, wodurch ein Paket als “ungewöhnlich” eingestuft werden kann. Beim Modul Anomaly Detection erfolgt dies aufgrund von statistischen Daten die durch Überwachung des normalen Datenverkehrs gesammelt werden –

	Netzwerkpakete mit ungewöhnlichen Eigenschaften werden dann protokolliert.
856	Portscan detected
	Ein Portscan wurde entdeckt. Weitere Informationen erhalten Sie in der Notification E-Mail.
857	Portscan detected – Event buffering activated
	Der Ereignispuffer wurde aktiviert. Weitere Intrusion-Protection-Ereignisse werden gesammelt und an Sie abgesendet, sobald die Sammelperiode abgeschlossen ist. Wenn weitere Ereignisse auftreten, wird diese Periode ausgedehnt.

CRIT:

025	License usage: Exceeding 100% of user count on Astaro Security Gateway
	Lizenznutzung: Die maximale Anzahl der möglichen Benutzer wird überschritten.
054	UPS power critical, system shutting down
	Die Spannungsversorgung des UPS-Geräts neigt sich einem kritischen Wert. Das Sicherheitssystem wird heruntergefahren.
060	RAID degraded: hard disk replacement needed
	Es wurde ein Fehler auf dem RAID-Festplattensystem festgestellt. Bitte wechseln Sie schnellstmöglich die defekte Festplatte .... aus.
080	HA check: No link beat on interface – going down
	Die Überwachung des Firewall-Systems im Normal-Modus mittels Link Beat ist fehlgeschlagen. Die Überwachung mittels Link Beat wird abgeschaltet.

301 System Up2Date failed: Could not connect to Authentication Server(s)

Der Authentication-Server ist nicht erreichbar. Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

302 System Up2Date failed: Download of System Up2Date Packages failed

Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

305 System Up2Date: Wrong MD5sum for local System Up2Date Package

Die MD5-Prüfsumme des lokalen System-Up2Date-Pakets ist falsch. Bitte laden Sie ein neues Up2Date-Paket herunter. Die Up2Dates können unter http://download.astaro.com/asl/up2date heruntergeladen werden. Wenn sich das Problem wiederholt, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

306 System Up2Date failed: Wrong MD5sum for downloaded Up2Date Package

Die MD5-Prüfsumme des eingespielten System-Up2-Date-Pakets ist falsch. Bitte spielen Sie ein neues Up2Date-Paket ein. Wenn sich das Problem wiederholt, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

308 System Up2Date failed: Could not connect to Authentication server. Trying another on

Die Verbindung zum Authentisierungs-Server kann nicht aufgebaut werden.

309	System Up2Date failed: No Authentication server available Die Authentisierung ist fehlgeschlagen. Kein Authentisierungs-Server verfügbar.
320	System Up2Date failed: Invalid start parameters Der System-Up2Date-Prozess wurde mit den falschen Parametern gestartet. Wenn sich das Problem wiederholt, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
322	System Up2date: Next Up2Date installation locked by HA Das nächste System Up2Date wird durch HA abgeschlossen.
323	System Up2Date failed: Corrupt Up2Date package Ein beschädigtes System-Up2Date-Paket wurde entdeckt. Bitte starten Sie den Vorgang von neuem. Wenn sich das Problem wiederholt, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
324	System Up2Date failed: Invalid License Ihre Lizenz ist abgelaufen.
325	System Up2Date failed: License check failed Ihre Lizenz kann nicht geprüft werden. Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
333	System Up2Date failed: Internal error Das System-Update ist fehlgeschlagen. Setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

334	System Up2Date failed: Invalid syntax Das System-Update ist aufgrund einer ungültigen Syntax fehlgeschlagen. Setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
335	System Up2Date failed: Up2Date directory not readable Das System-Update ist fehlgeschlagen, da das Up2Date-Verzeichnis nicht gelesen werden kann. Setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
336	System Up2Date failed: No installation directory Das System-Update ist fehlgeschlagen, da kein Installations-Verzeichnis vorhanden ist. Setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
337	System Up2Date failed: Could not extract tar Die tar-Datei konnte nicht extrahiert werden. Bitte starten Sie den Vorgang von neuem. Wenn sich das Problem wiederholt, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
338	System Up2Date failed: Main Up2Date package not found Das System-Update ist fehlgeschlagen, da das Main-Up2Date-Paket nicht gefunden wurde. Bitte starten Sie den Vorgang von neuem. Wenn sich das Problem wiederholt, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

339	System Up2Date failed: Version conflict Das System-Update ist aufgrund eines Versionskonflikts fehlgeschlagen. Bitte setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
340	System Up2Date failed: Pre-Stop-Services script failed Das System-Update ist fehlgeschlagen. Wenn sich das Problem wiederholt, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
341	System Up2Date failed: Post-Stop-Services script failed Das System-Update ist fehlgeschlagen. Wenn sich das Problem wiederholt, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
342	System Up2Date failed: Pre-Start-Services script failed Das System-Update ist fehlgeschlagen. Wenn sich das Problem wiederholt, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
343	System Up2Date failed: Starting Services failed Die Dienste konnten nicht gestartet werden. Bitte setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

344 System Up2Date failed: Post-Start-Services script failed

Das System-Update ist fehlgeschlagen. Wenn sich das Problem wiederholt, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

345 System Up2Date failed: Error occured while running installer

Das System-Update ist fehlgeschlagen, da während der Ausführung des Installer ein Fehler aufgetreten ist. Bitte setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

346 System Up2Date failed: Installer stopped due to internal error

Der System-Update ist fehlgeschlagen, da der Install-Prozess aufgrund eines internen Fehlers gestoppt wurde. Bitte setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

347 System Up2Date failed: Started without rpm parameters

Der System-Update ist fehlgeschlagen, da der Install-Prozess ohne rpm-Parameter gestartet wurde. Bitte setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

348 System Up2Date failed: System Up2Date subscription expired

Der System-Update ist fehlgeschlagen, da Ihr System-Up2Date-Abonnement abgelaufen ist.

349	System Up2Date failed: No rpm package in Up2date package. Exiting now Der System-Update-Vorgang wurde abgebrochen, da im Up2Date-Paket kein rpm-Paket enthalten ist.
351	Pattern Up2Date failed: No Authentication Server available Der Authentication-Server konnte nicht ausgewählt werden. Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
353	Virus Pattern Up2Date failed: No Up2Date Server available Der Up2Date-Server ist nicht erreichbar. Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
354	Intrusion Protection Pattern Up2Date failed: No Up2Date Server available Der Up2Date-Server ist nicht erreichbar. Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
355	Spam Pattern Up2Date failed: No Up2Date Server available
361	Pattern Up2Date failed: Restart of Content Scanner failed Der Content Scanner konnte nicht wieder gestartet werden. Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.

362	Pattern Up2Date failed: MD5sum error occurred Ein Fehler in der MD5-Prüfsumme ist aufgetreten. Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
365	Pattern Up2Date failed: Can’t restart Content Scanner with backup pattern Der Pattern-Update ist fehlgeschlagen, da der Content Scanner mit den aktualisierten Pattern nicht gestartet werden kann. Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
366	Pattern Up2Date failed: Restarted Content Scanner with backup pattern Der Pattern-Update ist fehlgeschlagen, da der Content Scanner mit den aktualisierten Pattern nicht gestartet werden kann. Falls das Problem andauert, setzen Sie sich mit dem Support Ihres Sicherheitssystem-Anbieters in Verbindung.
712	System shut down due to full log file partition Die derzeit erreicht Auslastung der Partition wird in der Notification angezeigt. Um vorzubeugen, dass Log-Dateien verloren gehen, ist das Internet-Sicherheitssystem automatisch heruntergefahren. Prüfen Sie die Einstellungen im WebAdmin und löschen Sie zur Sicherheit manuell alte Log-Dateien.
850	Intrusion Protection Alert Es wurde ein Paket entdeckt, das evtl. Teil eines Intrusion-Versuchs sein kann. Die Regel hat diesen Angriff als höchste Priorität einge-

stuft. Weitere Informationen erhalten Sie in der Notification E-Mail.

851 Intrusion Protection Alert – Event buffering activated

Es wurde ein Paket entdeckt, das evtl. Teil eines Intrusion-Versuchs sein kann. Die Regel hat diesen Angriff als höchste Priorität eingestuft. Der Ereignispuffer wurde aktiviert. Weitere Intrusion-Protection-Ereignisse werden gesammelt und an Sie abgesendet, sobald die Sammelperiode abgeschlossen ist. Wenn weitere Ereignisse auftreten, wird diese Periode ausgedehnt. Weitere Informationen erhalten Sie in der Notification E-Mail.

852 Intrusion Protection Alert

Es wurde ein Paket entdeckt, das evtl. Teil eines Intrusion-Versuchs sein kann. Die Regel hat diesen Angriff als höchste Priorität eingestuft und hat das Datenpaket automatisch abgefangen. Bei dieser Intrusion-Protection-Regel kann im WebAdmin zwischen den Aktionen „Alert only (nur alarmieren)“ und „Drop (abfangen)“ umgeschaltet werden. Weitere Informationen erhalten Sie in der Notification E-Mail.

853 Intrusion Protection Alert – Event buffering activated

Es wurde ein Paket entdeckt, das evtl. Teil eines Intrusion-Versuchs sein kann. Die Regel hat diesen Angriff als höchste Priorität eingestuft und hat das Datenpaket automatisch abgefangen. Der Ereignispuffer wurde aktiviert. Weitere Intrusion-Protection-Ereignisse werden ge-

sammelt und an Sie abgesendet, sobald die Sammelperiode abgeschlossen ist. Wenn weitere Ereignisse auftreten, wird diese Periode ausgedehnt. Bei dieser Intrusion-Protection-Regel kann im WebAdmin zwischen den Aktionen „Alert only (nur alarmieren)“ und „Drop (abfangen)“ umgeschaltet werden. Weitere Informationen erhalten Sie in der Notification E-Mail.

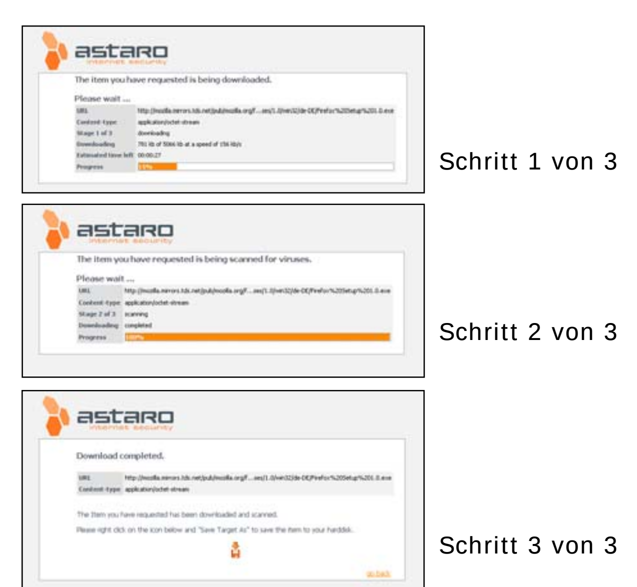
860 Intrusion Protection Alert - Buffered Events

Nach der Aktivierung des Ereignispuffers wurden weitere Intrusion-Protection-Ereignisse gesammelt. In der angehängten Datei ist ein Auszug aus den gesammelten Ereignisse enthalten. Eine komplette Liste mit Ereignissen wurde in den Intrusion Protection Log Files gespeichert.

5.10.3.3. HTTP Proxy Meldungen

Die folgenden Informationen und Fehlermeldungen werden vom HTTP-Proxy verschickt:

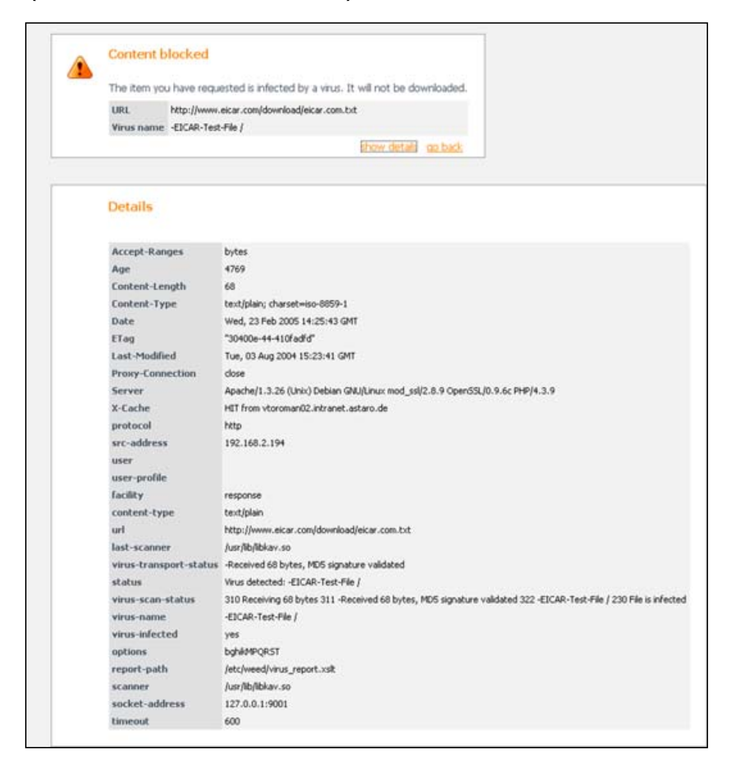
Download-Verlauf:



Internetseite wurde vom *Virus Protection for Web* blockiert:



Internetseite wurde vom *Virus Protection for Web* blockiert (detaillierte Informationen):



Accept-Ranges	bytes
Age	4769
Content-Length	68
Content-Type	text/plain; charset=iso-8859-1
Date	Wed, 23 Feb 2005 14:25:43 GMT
ETag	"30400e-44-410fadfd"
Last-Modified	Tue, 03 Aug 2004 15:23:41 GMT
Proxy-Connection	close
Server	Apache/1.3.26 (Unix) Debian GNU/Linux mod_ssl/2.8.9 OpenSSL/0.9.6c PHP/4.3.9
X-Cache	HIT from vtoroman02.intranet.astaro.de
protocol	http
src-address	192.168.2.194
user	
user-profile	
facility	response
content-type	text/plain
url	http://www.eicar.com/download/eicar.com.txt
last-scanner	/usr/lib/libkav.so
virus-transport-status	-Received 68 bytes, MD5 signature validated
status	Virus detected: -EICAR-Test-File /
virus-scan-status	310 Receiving 68 bytes 311 -Received 68 bytes, MD5 signature validated 322 -EICAR-Test-File / 230 File is infected
virus-name	-EICAR-Test-File /
virus-infected	yes
options	bghikMPQRST
report-path	/etc/weed/virus_report.xslt
scanner	/usr/lib/libkav.so
socket-address	127.0.0.1:9001
timeout	600

Internetseite wurde vom *Surf Protection* blockiert (detaillierte Informationen):



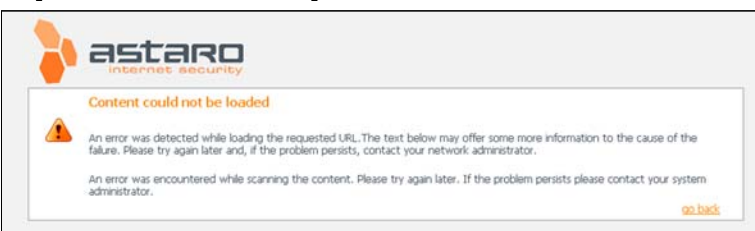
Details

url	http://www.heise.de/
method	GET
protocol	http
user-profile	profile_0_request
category-number	26
category-name	General News / Newspapers / Magazines
category-number	35
category-name	IT Security / IT Information
last-scanner	/usr/lib/libcofs.so
Reject-Subject	Blocked by Surf Protection
Unallowed-category	General News / Newspapers / Magazines
reason	URL category 'General News / Newspapers / Magazines' not allowed
Unallowed-category	IT Security / IT Information
reason	URL category 'IT Security / IT Information' not allowed
Host	www.heise.de
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Accept	text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language	en-ca,en-us;q=0.7,en;q=0.3
Accept-Charset	UTF-8,*
Keep-Alive	300
Proxy-Connection	keep-alive
Cookie	Hardware-Preisvergleich%20Cookie%20V0.0=neu&default; VisID=ID&MTEyNDM1NDQ3MC4xODc1OSwxMjcuMC4wLjEsNTIwMy4wMjYzMDcwNjA0NQ%3D%3D
Proxy-authorization	Basic LTpwcHBwCg==
Content-type	text/html

Internetseite wurde von der Funktion *URL Blacklist* geblockt:



Allgemeine Fehlermeldung:



5.11. Online Help/User Manual

Im Menü **Online Help** stehen Ihnen neben **Online Help** drei weitere Funktionen zur Verfügung.

5.11.1. Search

Mit Hilfe dieser Funktion wird im **WebAdmin** und in **Online Help** nach dem von Ihnen eingegebenen Begriff gesucht und der Begriff wird in einem separaten Fenster angezeigt.

Suche starten:

1. Öffnen Sie im Verzeichnis **Online Help** das Menü **Search**.
2. Geben Sie in das Eingabefeld **Search Term** den Begriff ein.
3. Um die Suche zu starten, klicken Sie auf die Schaltfläche **Start**.

Falls der Begriff im **WebAdmin** oder in **Online Help** geführt wird, liefert das Ergebnis folgende Infos:

- Pfad zur entsprechenden Funktion im **WebAdmin**
- Link zum gesuchten Begriff in **Online Help**
- Informationen zur Funktion oder die Texte aus der Online-Hilfe mit dem gesuchten Begriff

5.11.2. Glossary

In diesem Verzeichnis entspricht die Struktur der Begriffe ihrer Zuteilung im **WebAdmin**. Durch einen Klick auf die Begriffe erhalten Sie einen Überblick der Funktionen in diesem Verzeichnis.

5.11.3. User Manual



Im Menü **User Manual** können Sie die aktuelle Version des Benutzerhandbuchs herunterladen. Zum Öffnen des Benutzerhandbuchs benötigen einen PDF Reader (z. B. Adobe Reader).

5.12. Firewall verlassen (Exit)

Wenn sie den Browser mit einer offenen **WebAdmin**-Session schließen ohne den **WebAdmin** über **Exit** zu verlassen, so bleibt die letzte Session bis zum Ablauf des Time-outs aktiv.

In solch einem Fall können Sie sich erneut am **WebAdmin** anmelden. Es wird ein Bildschirm angezeigt, der Sie darüber informiert, dass bereits ein anderer Administrator eingeloggt ist. Sie können mit der Schaltfläche **Kick** die andere Session beenden und sich selbst wieder einloggen. Falls Sie damit die WebAdmin-Session eines anderen Administrators beenden, sollten sie im Eingabefeld für „Type reason here“ den Grund für die Übernahme der Session angeben.

Glossar

ARP

Das **Address Resolution Protocol** (**ARP**) dient dazu, für einen Host, dessen IP-Adresse bekannt ist, die zugehörige Ethernet-Adresse zu ermitteln. Der Sender verschickt hierzu per Broadcast ein ARP-Paket und wartet darauf, dass die Ethernet-Adresse wieder zurückgeschickt wird.

Broadcast

Die Adresse, an die sich ein Rechner wendet, wenn er alle Rechner im gleichen Subnetz ansprechen will.
Beispiel: Bei einem Netzwerk mit der IP-Adresse 192.168.2.0 und der Netzwerkmaske 255.255.255.0 wäre ein Broadcast die Adresse 192.168.2.255.

Client

Ein Client ist ein Programm, das über ein Netzwerk mit einem Server kommuniziert um den von ihm zur Verfügung gestellten Dienst zu nutzt.
Beispiel: Netscape ist ein WWW-Client, mit dessen Hilfe man Informationen von einem WWW-Server abrufen kann.

Client-Server Prinzip

Nach dem Client-Server Prinzip gestaltete Anwendungen verwenden auf der Benutzerseite ein Clientprogramm (Client), das mit einem bestimmten Dienstrechner im Netz (Server) Daten austauscht. Der Server ist dabei i.d.R. für die Datenhaltung zuständig, während der Client die Präsentation dieser Daten und die Interaktion mit dem Benutzer übernimmt. Dazu bedienen sich Client und Server eines

genau definierten Protokolls. Alle wichtigen Anwendungen im Internet (z.B. WWW, FTP, News) basieren auf dem Client-Server Prinzip.

DNS

Dank des Domain Name Systems (auch: Domain Name Service) kann der Anwender statt der rechnerfreundlichen IP-Nummer den menschenfreundlicheren Namen, bzw. Aliase, verwenden. Für die Umsetzung von Nummer nach Name sorgen die Nameserver. Jede am Internet angeschlossene Institution muss mindestens zwei voneinander unabhängige Nameserver betreiben, die über Namen und Nummern dieser Institution Auskunft geben können. Zusätzlich gibt es für jede Top-Level Domain einen Nameserver, der über eine Liste aller nachgeordneten Nameserver dieser Domain verfügt.

Das Domain Name System stellt also eine verteilte, hierarchische Datenbank dar. Im Normalfall fragt jedoch nicht der Benutzer selbst die Datenbank ab, sondern die Netzanwendung (z. B. Netscape) mit der er gerade arbeitet.

Dual-Homed Gateway

Man geht von einer Maschine ohne IP-Forwarding aus, die mit einem Netzwerkinterface Kontakt zum lokalen Netzwerk bzw. zum internen Teil einer Firewall besitzt und die mit einem zweiten Netzwerk-Interface mit dem externen Teil einer Firewall bzw. dem Internet verbunden ist. Aufgrund des fehlenden IP-Forwarding müssen alle Verbindungen über dieses Dual-Homed Gateway weitergeleitet werden.

Firewall

Eine Firewall dient der Abschirmung und damit dem Schutz eines (Teil-) Netzwerks (z. B. Astaro) von einem anderen Netzwerk (z. B. dem Internet). Der gesamte Netzwerkverkehr geht über die Firewall, wo er reguliert und reglementiert werden kann.

Header

Im Allgemeinen ein Bereich am Anfang bzw. am Kopf von Dateien, in dem grundsätzliche Informationen über diese Datei gespeichert sind. Im Speziellen ist es der Teil einer E-Mail oder einer Usenet-Nachricht, die Informationen über Inhalt, Absender und Datum gibt.

Host

In Client-Server-Architekturen bezeichnet man als Host den Rechner, auf dem die Server-Software läuft. Dabei können auf einem Host mehrere Server laufen, zum Beispiel ein FTP- und ein E-Mail-Server. Auf einen Host kann man mit Hilfe von Clients zugreifen, zum Beispiel mit einem Browser oder einem E-Mail-Programm. Da der Ausdruck **Server** außer für das entsprechende Programm (also die Software) auch für den Rechner verwendet wird, auf dem das Programm läuft (also die Hardware), wird in der Praxis nicht klar zwischen Server und Host unterschieden.

In der Datenfernübertragung bezeichnet man denjenigen Rechner als Host, von dem Daten (wie FTP-Dateien, News, WWW-Seiten) abgerufen werden. Ein Host wird im Internet auch als **Node** (Knoten) bezeichnet.
Auf einem Internet-Host (im Unterschied zum **Localhost**) kann man (zum Beispiel über Telnet) auch aus der Ferne arbeiten (Remote Access).

ICMP

Neben dem **IP-Protokoll** gibt es eine Variante mit speziellen Funktionen. Das **Internet Control Message Protocol (ICMP)** wird zur Übermittlung von Kontrollinformationen zwischen aktiven Netzwerkkomponenten oder Rechnern verwendet. Den meisten Anwendern sind die ICMP-Typen Echo (Typ 8) und Echo Reply (Typ 0) im Zusammenhang mit dem Programm **ping** bekannt. Empfängt ein Rechner ein ICMP-Echo-Paket, so muss sein IP-Stack ein ICMP-Reply-

Paket an den Absender zurückschicken. Man macht dies mit dem Programm ping, um festzustellen, ob eine andere Netzwerkkomponente über IP zu erreichen ist.

IP

Das **Internet Protocol** ist das Basisprotokoll für die Datenübertragung im Internet, das seit 1974 nahezu unverändert in Gebrauch ist. Es regelt den Verbindungsauf- und -abbau sowie die Fehlerkennung. Durch Verwendung von **NAT** und **Masquerading** können private Netzwerke auf offizielle IP-Adressen gemappt werden – auf diese Weise wird der Ipv4-Adressraum noch lange ausreichen.

IP-Adresse

Jeder Host besitzt eine eindeutige IP-Adresse, vergleichbar mit einer Telefonnummer. Eine IP-Adresse besteht aus vier durch Punkte voneinander getrennte dezimale Ziffern. Die möglichen Ziffern sind 0 bis einschließlich 255.
Beispiel: Eine mögliche IP-Adresse ist 192.168.2.15.

Zu jeder IP-Adresse gehört mindestens ein IP-Name der Form `hostname[[.subdomain]s].domain`, z. B. `kises.rz.uni-konstanz.de`. Hiermit wird ein Rechner namens `kises` bezeichnet, der in der Sub-Domain `rz` der Sub-Domain `uni-konstanz` der Domain `de` steht. Wie bei IP-Adressen, werden die einzelnen Namensteile durch einen Punkt voneinander getrennt. Anders als bei IP-Adressen jedoch, sind IP-Namen nicht auf vier Stellen beschränkt. Außerdem können einer IP-Adresse mehrere IP-Namen zugeordnet sein, man spricht dann von Aliasen.

Masquerading

Dynamisches **Masquerading** ist eine Funktion, die auf der NAT-Technologie basiert. Mit dieser Funktion kann das gesamte lokale Netzwerk (LAN) über eine einzelne öffentliche IP-Adresse nach außen kommunizieren.

Beispiel: Der Rechner eines Mitarbeiters mit der IP-Adresse 192.168.2.15 steht in einem maskierten Netzwerk. Allen Rechnern in seinem Netzwerk wird eine einzige, offizielle IP-Adresse (z. B. 199.199.199.1) zugeordnet, d. h. wenn er nun eine HTTP-Anfrage in das Internet startet, wird seine IP-Adresse durch die IP-Adresse der externen Netzwerkkarte ersetzt. Damit enthält das ins externe Netzwerk (Internet) gehende Datenpaket keine internen Informationen. Die Antwort auf die Anfrage wird von der Firewall erkannt und auf den anfragenden Rechner weitergeleitet.

nslookup

Ein Unix Programm zur Abfrage von Nameservern. Die Hauptanwendung ist die Anzeige von IP-Namen bei gegebener IP-Nummer, bzw. umgekehrt. Darüber hinaus können aber auch noch andere Informationen wie z.B. Aliase angezeigt werden.

Port

Während auf IP-Ebene nur die Absender- und Zieladressen zur Übertragung verwendet werden, müssen für TCP und UDP weitere Merkmale eingeführt werden, die eine Unterscheidung der einzelnen Verbindungen zwischen zwei Rechnern erlauben. Dies sind die Portnummern. Eine Verbindung auf TCP und UDP-Ebene ist damit durch die Absenderadresse und den Absenderport sowie die Zieladresse und den Zielport eindeutig identifiziert.

Protokoll

Ein Protokoll ist ein klar definierter und standardisierter Satz von Regeln, mit deren Hilfe ein Client und ein Server miteinander kommunizieren können. Bekannte Protokolle und die damit betriebenen Dienste sind z. B. HTTP (WWW), FTP (FTP) und NTP (News).

Proxy (Application Gateway)

Die Aufgabe eines Proxy (Application Gateways) ist die vollständige Trennung von Kommunikationsverbindungen zwischen dem externen Netzwerk (Internet) und dem internen Netzwerk (LAN). Zwischen einem internen System und einem externem Rechner kann keine direkte Verbindung existieren.
Die Proxies arbeiten vollständig auf der Applikationsebene. Firewalls, die auf Proxies basieren, benutzen ein Dual-Homed Gateway, das keine IP-Pakete weiterleitet. Die Proxies, die auf dem Gateway als spezialisierte Programme ablaufen, können nun Verbindungen für ein spezielles Protokoll entgegennehmen, die übertragenen Daten auf Applikationsebene verarbeiten und anschließend weiterleiten.

RADIUS

RADIUS steht für Remote Authentication Dial In User Service. RADIUS ist ein Protokoll, mit dem ein Router Informationen für die Benutzerauthentifizierung von einem zentralen Server abfragen kann.

Router (Gateway)

Ein Router ist ein Vermittlungsrechner, der eine intelligente Wegewahl für die Netzwerkpakete auswählt. Ein Gateway ist streng genommen etwas anderes als ein Router, aber im Zusammenhang mit TCP/IP sind beide Begriffe synonym. Wenn man Verbindungen über das eigene Netzwerk hinaus aufbauen möchte, muss man dem eigenen Rechner diesen Router (Gateway) bekannt machen. Gewöhnlich wird

die höchste oder die niedrigste Adresse verwendet, z. B. im Netzwerk 192.168.179.0/24 die Adresse 192.168.179.254 oder 192.168.179.1.

Server

Ein Server ist ein Rechner im Netz, der besondere, i.d.R. standardisierte, Dienste anbietet, z.B. WWW, FTP, News, usw. Um diese Dienste nutzen zu können, brauchen Sie als Anwender einen für den gewünschten Dienst passenden Client.

SIP

Das T**Session Initiation ProtocolT** (**SIP**) ist ein Signalisierungsprotokoll zum Aufbau, zur Modifikation und zum Beenden von Sitzungen zwischen zwei oder mehreren Kommunikationspartnern. Das textorientierte Protokoll basiert auf HTTP und kann Signalisierungsdaten per TCP oder UDP über IP-Netzwerke übertragen. Es bildet damit u. a. die Grundlage für Voice-over-IP-Videotelefonie (VoIP) und Multimedia-Dienste in Echtzeit. Im Multimedia-Subsystem ist SIP die Basis für Verbindungen, die zwischen Mobilfunkteilnehmern über ein IP-Netzwerk hergestellt werden. Dies ermöglicht kostengünstige Kommunikationsformen wie Push to Talk over Cellular. SIP ist in den RFCs 3261-3265 definiert.

SOCKS

SOCKS ist ein Proxyprotokoll, das dem Anwender erlaubt, eine Punkt-zu-Punkt-Verbindung zwischen einem internem und einem externem Rechner über das Internet zu erstellen. SOCKS, oft auch Firewall Transversal Protocol genannt, existiert derzeit in der Version 5 und klinkt sich auf Clientseite in die SOCKS-Aufrufe der Programme ein.

Subnet Mask

Die Subnet Mask oder Netzwerkmaske gibt an, in welche Gruppen die IP-Adressen eingeteilt sind. Aufgrund dieser Einteilung werden einzelne Rechner einem Netzwerk zugeordnet.

UNC-Pfad

Mit Hilfe eines T**Universal Naming Convention**-Pfadnamen (UNC-Pfad), z. B. \\Servername\Freigabename kann man manuell eine Verknüpfung zu einem Netzlaufwerk erstellen.

Voice over IP

Voice over IP (**VoIP**) ist der Sammelbegriff für Sprachvermittlung über IP-Netzwerke. Neben der Sprachvermittlung sind auch Video und interaktive Multimedia-Dienste möglich. Um derartige Systeme realisieren zu können, setzt man Gatekeeper ein, deren Funktionen in einer Reihe von Standards definiert sind. Relevant sind vor allem die Standards H.323 und H.225, das RAS-Protokoll und das H.225-Handshake-Verfahren-Verfahren, RTP und RTCP.

Index

ACC 410
Accounting
  Einleitung 220
  Netzwerkkarte
    hinzufügen/entfernen.. 221
Administrator e-mail addresses
 48
Akustische Signale
  Beep, 5 mal................. 132
  Endlos-Beep 132
Anti-Virus Engines
  Astaro AV Engine............77
  Einleitung......................77
  Open Source AV Engine ...77
ARM
  ARM Remote Connection 414
  Historical ARM Log Files. 413
  Transfermethode 414
Astaro Command Center (ACC)
  410
Astaro Report Manager (ARM)
  411
Astaro Secure Client
  Client Parameters......... 385
  Profil-Import................ 383
Backup
  Einleitung......................69
  E-Mail Backup File
    generieren 75
  E-Mail Backup File
    verschlüsseln...............74
  E-Mail-Adressen bearbeiten
   76
  installieren, manuell........71
  installieren, mittels USB-
    Speicher 70
  manuell generieren.........72
Benutzer
  Definitionen editieren.... 149
  Definitionen löschen......149
  Einleitung....................146
  Filter...........................148
  filtern 148
  lokale Benutzer hinzufügen
   147
Bounce...........................349
Bridging
  Ageing Timeout 193
  Allow ARP Broadcasts 193
  Bridge Options 193
  definieren....................191
  Einleitung....................191
  Garbage Collection Intervall
   193
  Netzwerkkarte hinzufügen
   192
  Netzwerkkarte löschen ..192
Broadcast
  auf ein Netzwerksegment
   255
  auf gesamtes Internet...254
Browser MS Explorer
  Proxy-Verwendung
    umgehen..................269
Browser Netscape
  Proxy-Verwendung
    umgehen..................270
Certifications....................129
Common Criteria Certification
 129
Connection Tracking Helpers
  Einleitung....................260
  Helper-Module laden 261
Connection Tracking Table..267
Content Filter 324
Current System NAT Rules .266
Current System Packet Filter
  Rules 266

DHCP Relay
  konfigurieren 207
DHCP Server
  Current IP Leasing Table 211
  DNS-Server, Gateway-IP und WINS-Server zuweisen................... 209
  konfigurieren 208
  Statische Adresszuweisung (Static Mappings) 210
DHCP Service
  Einleitung.................... 206
Dienste
  Definitionen editieren.... 146
  Definitionen löschen...... 146
  Dienstgruppe definieren 144
  Einleitung.................... 141
  Filter 145
  filtern 145
  hinzufügen 142
DNS
  konfigurieren 337
Dynamic DNS
  Einleitung.................... 153
  Host definieren............. 153
Exit 466
Factory Reset 54
Fehler
  Ursachen................30, 158
Firewall
  Die Technologie..............12
  Lizensierung 56
Firewall Hostname 152
General System Settings......48
Generic
  konfigurieren 339
Glossar
  ARP........................... 467
  Broadcast.................... 467
  Client 467
  Client-Server Prinzip 467
  DNS 468
  Dual-Homed Gateway ... 468
  Firewall 468
  Header........................ 469
  Host 469
  ICMP 469
  IP.............................. 470
  IP-Adresse................... 470
  Masquerading 471
  nslookup 471
  Port 471
  Protokoll 472
  Proxy.......................... 472
  RADIUS....................... 472
  Router 472
  Server 473
  SIP............................ 473
  SOCKS........................ 473
  Subnet Mask................ 474
  UNC-Pfad 474
  Voice over IP 474
Glossary 465
Header 324
High Availability................ 122
High Availability-System
  installieren 124
Hochverfügbarkeit............. 122
Hostname 152
http
  Domain Profile editieren 312
HTTP
  ActiveDirectory/NT-Domain-Membership-Modus..... 272
  Advanced 277
  Global Settings............. 271
  HTTP-Proxy-Meldungen . 462
  Operation Modes 271
  Parent Proxy 276
  Parent-Proxy definieren . 276
  Proxy einschalten 273
  Spyware Protection 279, 292
  Standard-Modus 271
  Transparent-Modus 272

User Authentication-Modus 272
ICMP
Einleitung 256
Firewall forwards ping ... 259
Firewall forwards Traceroute 258
Firewall is ping visible ... 259
Firewall is Traceroute visible 258
ICMP Forwarding 257
ICMP on Firewall........... 257
Log ICMP Redirects 257
Ping on firewall 259
Ping Settings 259
Traceroute from Firewall 259
Traceroute Settings 258
ICMP Flood Protection
einschalten/ausschalten 239
ICMP Flood Protection........ 239
ICSA Labs Certification 131
Ident
Einleitung 346
Forward Connections..... 346
Installation
Anleitung 25
Einleitung......................20
Konfiguration 30
Software 25
Version 4.0x auf 5.0 aktualisieren................20
Vorbereitung..................25
Interfaces
Current Interface Status 155
Hardware List 157
MTU Size......164, 172, 178, 184, 189
Interfaces....................... 154
Intrusion Protection
Advanced 241
Anomaly Detection 223
DoS/Flood Protection 234
Einleitung 223
Global Settings.............223
IPS-Regel-Übersicht 226
Lizensierung 56
Notification Levels 224
Pattern Up2Date.............66
Regel setzen 229
Rules 226
IPSec VPN
Advanced 394
AH-Protokoll 361
CA Management 389
Client/Host-Zertifikat erstellen....................391
Connections.................365
Einleitung 355
Global IPSec Settings 365
IPSec..........................359
IPSec Connection Status 366
IPSec Connections 366
IPSec Modi 360
IPSec System Information 367
IPSec-Protokolle 361
konfigurieren 368
L2TP over IPSec 386
Lizensierung 56
Local IPSec X.509 Key ...379
Local Keys 379
Manual Keying 362
Policies 374
Policy konfigurieren 374
PSK Authentication 381
Remote Key definieren ..383
Remote Keys 382
RSA Authentication 380
Schlüsselverwaltung......362
Transport Modus 360
Tunnel Modus 360
User Config Download ...382
VPN Routes..................367
VPN Status 367

L2TP over IPSec
- L2TP over IPSec Client Parameters................ 388
- L2TP over IPSec IP Pool. 387
- L2TP over IPSec Settings 386

Licensed Users 59
Licensing 56
Licensing Information 59
Lizenzierung 56
Load Balancing
- Einleitung 204
- Regel definieren 205
- Regel editieren............. 206
- Regel löschen 206

Local Logs
- Browse 422
- Einleitung 417
- filtern 425
- Filters 425
- Local Log File Archive.... 418
- Local Log File Level konfigurieren 418
- Local Log File Query...... 421
- Log Files 426
- Log Files löschen (nach Zeitspanne)............... 418
- Remote Log File Archive 419
- Settings 417
- Suchanfrage starten 421
- Wipe Local Log File Archives 421

Local Users 85
Log Files
- Accounting Data........... 426
- Admin Notifications....... 426
- Boot Messages 426
- Configuration Daemon... 426
- Content Filter............... 426
- DHCP Server................ 426
- DNS Proxy................... 426
- Fallback Messages 427
- High Availability 427
- HTTP accessed sites 427
- HTTP blocked sites........427
- HTTP Daemon 427
- HTTP Proxy..................427
- Intrusion Protection 427
- Intrusion Protection System 427
- IPSec VPN 427
- Kernel Messages...........427
- License Information 428
- Local Logins.................428
- Logging Subsystem.......428
- MiddleWare..................428
- Network Accounting Daemon 428
- Packet Filter.................428
- POP3 Proxy..................428
- Portscan......................428
- PPP Daemon 429
- PPPoA 429
- PPPoE 429
- PPTP Daemon 429
- Remote Configuration Manager....................429
- Selfmonitoring 429
- SIP Proxy 430
- SMTP Proxy 430
- SOCKS Proxy 430
- SSH Daemon 430
- System Log Messages ...430
- Up2Date Messages 430
- Uplink Failover Messages430
- User Authentication Daemon 430
- WebAdmin...................431

Log Files Settings
- Level definieren............419

Log FTP Data Connections..264
Log Unique DNS Requests..264
Logging Options................264

Masquerading
Regel definieren 203
Regel editieren............. 204
Regel löschen 204
Masquerading Einleitung 202
Microsoft Outlook
Regeln erstellen 325
Mozilla Firefox
Proxy-Verwendung
umgehen 270
NAT
Einleitung.................... 198
Regel editieren............. 202
Regel löschen 202
Regel setzen................ 200
Networks
Filters 140
Networks........................ 134
Netzwerke
Definitionen editieren 141
Definitionen löschen...... 141
Einleitung.................... 134
Filter 140
filtern 140
Host hinzufügen 135
IPSec-Benutzergruppen
definieren.................. 139
Netzwerk hinzufügen 136
Netzwerkgruppen definieren
.... 138
Netzworke
DNS-Server hinzufügen . 137
Notification 152
Notification Codes
CRIT.......................... 452
INFO 431
WARN........................ 445
Notification Codes 431
Novell eDirectory
eDirectory-Server einstellen
................................86
Einleitung.....................86
Novell eDirectory
User/Group/Container-
based Access Control 89
Single Sign-on 88
WebAdmin konfigurieren..87
Packet Filter
Advanced 260
Packet Filter Live Log
Einleitung 265
Filter setzen/zurücksetzen
..............................266
Paketfilterregeln
Einleitung 243
Filter..........................251
filtern 251
Gruppe hinzufügen/editieren
..............................249
Regel aktivieren,
deaktivieren 249
Regel editieren 250
Regel löschen...............250
Regelsatztabelle 248
Regelsatztabelle sortieren
..............................250
Reihenfolge ändern 250
setzen........................245
Zeitsteuerung 250
Password-Restriktionen.. 55, 85
Pattern Up2Date
installieren, automatisch..67
installieren, manuell........66
Phishing Protection.....294, 349
Ping
starten........................222
Ping Check
Einleitung 221
POP3
Content Filter 332
Expressions Filter 335
File Extension Filter.......335
konfigurieren 331
Message Style 335

Spam Protection 332
Spam Sender Whitelist .. 334
Virus Protection 332
Portscan Detection
einschalten/ausschalten 232
Portscan Detection 230
PPTP VPN
DHCP Settings 215, 388
Einleitung 212
MS-Windows-2000-Szenario
.... 216
PPTP Client Parameters . 215
PPTP IP-Pool 214
PPTP VPN Access 212
Protocol Handling 261
Protokolle
AH 142, 143
ESP 142, 143
IP 143
TCP 141
UDP 141
Proxy
DNS 336
Einleitung 268
Generic 338
HTTP 269
Ident 346
POP3 330
Proxy Content Manager . 347
SIP 340
SMTP 304
SOCKS 344
Proxy Content Manager
Age 348
Automatic Cleanup 352
blockierte Categories 403
blockierte Seiten 403
Daily Spam Digest 353
deferred/zurückgestellt . 348
erlaubte Seiten 403
filtern 351
Filters 351
Global Actions 350
Mail-ID 347
permanent
error/andauernder Fehler
.... 348
quarantined/gesperrt 348
Recipient(s) 349
Sender 349
Status 348
Type 347
Quality of Service (QoS) 252
RAID-Festplattensystem 407
Remote Management 410
Remote Syslog Server
Einleitung 81
Reporting
Accounting
Netzwerk definieren 405
Accounting 405
Administration 398
Advanced 407
Content Filter 402
DNS 402
Executive Report 404
Hardware 400
HTTP Proxy Usage 403
Intrusion Protection 402
Network 401
Packet Filter 401
PPTP/IPSec VPN 402
RAID Status 407
SIP 403
System Information 408
Virus Protection 399
Restart 132
Routing
Einleitung 194
Kernel Routing Tabelle .. 195
Policy Routes 196
Policy Routes definieren . 196
Statische Routes 194

Statische Routes definieren 194
Rules 243
Schnittstellen
Aktuelle Übersicht 155
Downlink Bandwidth (kbits) .. 163, 171, 177, 184, 189
Einleitung.................... 154
Ethernet-Netzwerkkarte 159
Hardware-Übersicht...... 157
Monitor Interface Usage 162
Notify when downlink usage below (%)................. 164
Notify when downlink usage exceeds (%)............. 164
Notify when uplink usage below (%)................. 163
Notify when uplink usage exceeds (%)............. 163
PPP over Serial Modem einrichten.................. 185
PPP over Serial Modem Line 185
PPPoA-DSL einrichten.... 180
PPPoE-DSL einrichten.... 174
PPPoE-DSL-Verbindung 174, 179
Proxy ARP 160
QoS-Status...162, 171, 177, 183, 189
Transparent (Bridging) Mode 157
Uplink Bandwidth (kbits) .. 163, 171, 177, 183, 189
Uplink Failover on Interface 161, 175, 182, 187
Virtual LAN 168
Virtual LAN einrichten ... 170
Zusätzliche Adresse 166
zusätzliche Adresse zuweisen................... 166
Search
Suche starten 465
Search 465
Secure Shell................. 52, 54
Services
Filters 145
Services 141
Settings............................48
Shut down 132
Shut down/Restart 132
SIP
SIP-Proxy definieren 341
SMTP
Advanced Settings 329
Content Filter 315
Deny RCPT Hacks 310
Domain Groups 307
Domain hinzufügen und editieren 307
Domain-Groups-Tabelle . 306
DoS Protection 329
Einleitung 304
Expression Filter 319
Feature Settings 314
File Extension Filter....... 317
konfigurieren 305
Max Message Size......... 329
MIME Error Checking..... 315
Outgoing TLS 329
Postmaster Address 305
Profiles-and-Domain-Group-Assignment-Tabelle 307
Route Target................ 308
Scan outgoing Messages 315
Sender Blacklist............ 308
SMTP Authentication 327
Spam Protection 320
Spam Recipient Whitelist323
Spam Sender Whitelist .. 322
SPF Fail Check 310
TLS-Verschlüsselung 329
Use BATV 310, 314

Use Greylisting 311, 314
Use RBL 309, 314
Use Smarthost 330
Verify Recipient 312
Verify Sender 312
Virus Protection 318

SNMP
Einleitung 79
Trap-Server zuweisen 80
Zugang erlauben 79

SOCKS
Benutzerauthentifizierung 345
konfigurieren 344

Spam Protection
Lizensierung 56
POP3 332
SMTP 320

Spoofing Protection 263

Spyware Protection
Die Technologie 292

Strict TCP Session Handling 261

Surf Protection
Block Spyware 292
Block suspicious and unkown sites 294
Categories 281, 291
Categories editieren 289
Custom HTML Content Removal 296
Einleitung 279
einschalten und Profile hinzufügen 297
File Extension Blocking . 295, 299
Lizensierung 56
Profile editieren 297
Profile zuweisen 303
Profile-Assignment-Tabelle 300
Profiles-Funktionen 291, 300
Profiles-Tabelle 290
Skip Authentication for Domains 280
Strip Embedded Objects 294
Strip Scripts 294
URL Blacklist 296
URL Whitelist 295
Whitelist Domains 280

SYN (TCP) Flood Protection
einschalten/ausschalten . 235

SYN (TCP) Flood Protection 234

System Information 265

System Time
automatisch synchronisieren 51
manuell einstellen 50

System Up2Date
einspielen, automatisch ... 62
einspielen, lokal 63
einspielen, manuell 62
installieren 64
installieren auf HA-Lösung 64

Systemvoraussetzungen
Administrations-PC 23
Beispielkonfiguration 23
Hardware 21

TCP Window Scaling 261

Time Events
Zeitintervall konfigurieren 151
Zeitintervall löschen 151

Time Settings 49

Transparent (Bridging) Mode 157

UDP Flood Protection
einschalten/ausschalten . 237

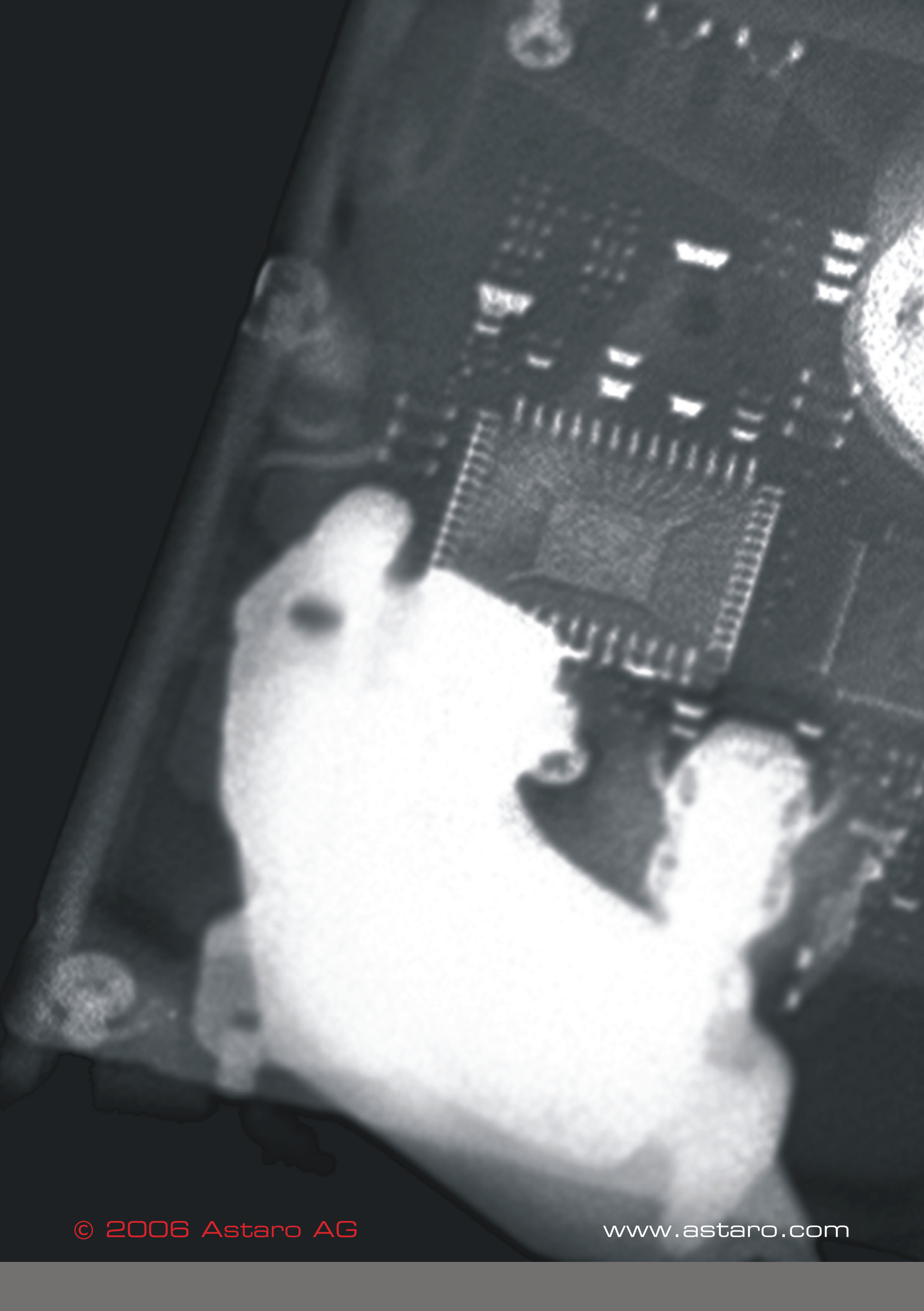
UDP Flood Protection 237

Up2Date Service
Einleitung 60
Lizensierung 56
Pattern Up2Date 66
System Up2Date 61

Upstream Proxy Server definieren....................68
Use Upstream HTTP Proxy68
UPS-Geräte-Support.....22, 399
Upstream-Proxy 60, 61, 68
Use external indicators 49
User Authentication
Active Directory/NT Domain Membership.................98
Active Directory/NT Membership einstellen 100
Einleitung......................83
LDAP einstellen 112
LDAP erweitert.............115
LDAP-Server................102
Microsofts IAS RADIUS einstellen 92
MS Active Directory-Server einstellen 104
Novell eDirectory-Server einstellen 110
NTLM...........................98
OpenLDAP-Server Konfigurieren.............111
RADIUS 91
SAM 96
SAM – NT/2000/XP einstellen 96
User Manual.....................466
Users
Filters.........................148
Users 146
USV 22
Validate Packet-Length 262
Virus Protection for E-Mail
Lizensierung 56
POP3 332
SMTP 318
Virus Protection for Web
Ein-/ausschalten...........291
Lizensierung 56
WebAdmin
Access and Authentication 117
Auswahlfeld 41
Auswahltabelle 42
Block Password Guessing 118
Bockierschutz für Loggin-Versuche einstellen.....118
Drop-down-Menü............43
Einleitung 20, 46
General Settings...........116
Hierarchiefeld.................43
HTTPS........................116
Info-Box.......................39
Kick 47
Menü 40
Online-Hilfe 45
Refresh 45
starten 47
Statusampel 40
Verzeichnis 40
WebAdmin Site Certificate..119
Zertifikat für WebAdmin
Einleitung 119
erstellen.....................120
installieren 121
Zertifizierungen 129

Notizen

Notizen



© 2006 Astaro AG
www.astaro.com